جمهوری اسلامی ایران

فرهنگستان زبان و ادب فارسی

انجمن رمز ایران
Iranian Society of Cryptology

ویرایش دوم

مجموعه واژه‌های مصوب

رمزشناسی

گروه واژه‌گزینی انجمن رمز ایران

کارگروه واژه‌گزینی رمزشناسی
فرهنگستان زبان و ادب فارسی

شهریورماه ۱۴۰۵

کارگروه واژه‌گزینی رمزشناسی:

جواد مهاجری

ترانه اقلیدس

مهشید دلاور

حبیب رستمی

هادی‌شهریارشاه‌حسینی

جواد شیخ‌زادگان

کارشناسان فرهنگستان زبان و ادب فارسی:

سمانه ملک‌خانی، محمدرضا حسینی، مرحوم فرزین غفوری

هیئت فنی:

نسرین پرویزی، علاءالدّین طباطبائی

شورای هماهنگی:

محمود ظریف، شکوه‌السادات میرفارسی

شورای واژه‌گزینی فرهنگستان زبان و ادب فارسی:

علی‌اشرف صادقی	غلامعلی حداد عادل	ژاله آموزگار
رضا منصوری	نسرین پرویزی	مرحوم احمد سمیعی (گیلانی)
محمدرضا بهاری	علاءالدّین طباطبایی	علی کافی
علی پورجوادی	محمدابراهیم ابوکاظمی	مهشید میرفخرایی
محمدتقی راشدمحصل	قطب‌الدّین صادقی	ابراهیم نقیب‌زادهٔ مشایخ
هوشنگ مرادی کرمانی	حسین معصومی همدانی	سیامک کاظمی
مرحوم عبّاس حُرّی	هوشنگ رهنما	مرحوم محمد خوانساری
ایران کلباسی	شهین نعمت‌زاده	زهره زرشناس

به نام خدا

پیش‌گفتار

توسعهٔ سریع دانش و فناوری رمز و امنیت فضای تولید و تبادل اطلاعات (افتا) ورود لغات و اصطلاحات متعددی از این حوزه را در زبان فارسی به دنبال داشته است. انجمن رمز ایران، با انتخاب زبان فارسی، به عنوان زبان علمی خود، گزینش و پیشنهاد واژه‌های مناسب فارسی برای لغات و اصطلاحات متداول بیگانه را در دستور کار خود قرار داده است. به این منظور گروه واژه‌گزینی انجمن در سال ۱۳۸۷ تشکیل شد. حاصل کار مستمر و سازمان‌یافتهٔ این گروه تدوین و انتشار ویرایش اول کتاب «واژه‌نامه و فرهنگ امنیت فضای تولید و تبادل اطلاعات (افتا)» در سال ۱۳۹۰ و ویرایش دوم آن در سال ۱۳۹۴ بوده است. در کنار این فعالیت، از اردیبهشت ماه سال ۱۳۸۹ همکاری گروه، با فرهنگستان زبان و ادب فارسی شکل گرفت و بر مبنای تفاهم‌نامه همکاری با فرهنگستان زبان و ادب فارسی، کارگروه رمزشناسی در این فرهنگستان تشکیل شد و طبق اصول و ضوابط فرهنگستان، کار واژه‌گزینی حوزه رمزشناسی و افتا به صورت مستمر ادامه یافت. نتیجه ارتباط و همکاری مستمر گروه واژه گزینی با فرهنگستان زبان و ادب فارسی و تشکیل حدود ۲۴۰ جلسه و بررسی بیش از ۱۰۰۰ واژه، منجر به تصویب حدود ۶۵۰ واژه در فرهنگستان زبان و ادب فارسی شده است که در دفاتر مختلف « فرهنگ واژه‌های مصوب فرهنگستان» منتشر شده است.

پس از انتشار نسخه اول مجموعه واژه‌های مصوب کارگروه رمزشناسی در سال ۱۴۰۲، و استقبال اساتید، دانشجویان، پژوهشگران و فعالان حوزه افتا، اینک ویرایش دوم مجموعه واژه‌های مصوب با افزودن ۵۲ واژه مصوب جدید و ویرایش جامع نسخه اول در اختیار عموم علاقه‌مندان قرار می‌گیرد.

در پایان بر خود لازم می‌دانم از اعضای محترم گروه: خانم‌ها دکتر ترانه اقلیدس، دکتر مهشید دلاور، و آقایان مهندس حبیب رستمی، دکتر هادی‌شهریار شاه‌حسینی و دکتر جواد شیخ‌زادگان، نمایندگان محترم فرهنگستان: خانم سمانه ملک‌خانی، آقایان دکتر محمدرضا حسینی، و مرحوم دکتر فرزین غفوری که با حضور مستمر و ایثارگونه خود، همچنین از آقایان دکتر محمدرضا عارف، دکتر غلامعلی حداد عادل، دکتر محمود سلماسی‌زاده و مجموعه اساتید، مدیران و کارشناسان انجمن رمز ایران و فرهنگستان زبان و ادب فارسی که با حمایت، راهنمائی و پشتیبانی خود، انجام و استمرار این فعالیت و تهیه این مجموعه ارزشمند را ممکن ساختند صمیمانه سپاس‌گذاری نمایم.

جواد مهاجری

مهر ۱۴۰۵

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	پی‌گیری‌پذیری	امکان ردگیری منحصربه‌فرد 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 سامانهٔ 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	فریب‌دهندهٔ فعال	هستاری که به منظور فریبکاری، یک پروتکل در حال اجرا را مختل می کند
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 رمزشده یا بازارسال (retransmit) آن در هر زمان دیگر یا وارد کردن متن جدید را انجام دهد

واژه بیگانه	معادل فارسی	تعریف
active penetration test	آزمون نفوذ فعال	آزمونی برای کاوش مرزهای محدودهٔ هدف و بررسی ضعف‌های امنیتی در محیط هدف، شامل آزمون‌های دارای عمق نفوذ بیشتر در قیاس با آزمون¬های نفوذ غیرفعال، با بهره‌گیری از ضعف‌های امنیتی ذاتی موجود در فناوری محیط هدف، خطاهای طراحی یا ضعف‌های موجود در پیکربندی
active wiretapping	خط‌شنود فعال	نوعی شنود خط برای تغییر داده‌های درحال‌مبادله با تأثیر بر جریان آن‌ها
adaptive adversary syn. dynamic adversary	مهاجم وفقی مت. مهاجم پویا	مهاجمی که در طول اجرای یک پروتکل تصمیم می‌گیرد که کدامیک از نهادهای های شرکت کننده در پروتکل را به عنوان نهاد تسخیر شده انتخاب کند
adaptive chosen ciphertext attack	حمله با متن رمز منتخب وفقی	نوعی حمله با متن رمز منتخب که در آن مهاجم قادر است ورودی به تابع رمزگذاری را براساس متن‌های رمز منتخب پیشین انتخاب کند
adaptive chosen message attack	حمله با پیام منتخب وفقی	نوعی حمله به طرح‌های امضا که در آن مهاجم به‌کمک امضاهای دریافتی بر روی تعدادی پیام منتخب اقدام به جعل امضا بر روی پیام موردنظر کند
adaptive chosen plaintext attack	حمله با متن اصلی منتخب وفقی	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

واژه بیگانه	معادل فارسی	تعریف
adversarial attack	حملهٔ خصمانه	

حمله‌ای که از طریق فضای تولید و تبادل اطلاعات صورت می‌گیرد و اهدافی مانند فروپاشیدن، ناکارآمدسازی، تخریب یا واپایش بدخواهانهٔ یک محیط یا زیرساخت محاسباتی یا تخریب درستی داده‌ها یا سرقت اطلاعات مورد واپایش را دنبال می کند

algebraic attack syn. algebraic cryptanalysis	حملهٔ جبری مت. تحلیل رمز جبری	

حمله‌ای که بر پایه حل معادلات جبری مستخرج از سامانهٔ رمز انجام می‌شود

algebraic cryptanalysis syn. algebraic attack	تحلیل رمز جبری مت. حملهٔ جبری	

حمله‌ای که بر پایه حل معادلات جبری مستخرج از سامانهٔ رمز انجام می‌شود

algebraic immunity degree	درجهٔ ایمنی جبری	

به ازای یک تابع بولی f ، برابر است با حداقل درجهٔ جبری توابع پوچ ساز f یا $1+f$ که به صورت زیر بیان می‌شود:

$$AI(f) = \min\{\deg(g)\,;\, g \neq 0, g \in AN(f) \cup AN(1+f)\}$$

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 درمورد 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 کدام‌یک از رازهاست؛ در این طرح افشا، به‌محض دریافت اطلاعات توسط کاربر دوم وی فرصت خود را برای کسب هرگونه اطلاعاتی دربارهٔ سایر رازها از دست خواهد داد

all-or-nothing encryption	رمزگذاری همه‌یاهیچ	

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 دانش‌صفر تقریباً کامل مت. اثبات ناتراوای آماری، اثبات دانش‌صفر آماری	

اثباتی که در آن، برخلاف حالت‌های کلی اثبات‌ناتراوا، توزیع مکالمات واقعی با توزیع مکالمات شبیه‌سازی‌شده از نظر آماری تمایزناپذیر است؛ یعنی فاصلهٔ آماری میان توزیع‌ها ناچیز است

واژه بیگانه	معادل فارسی	تعریف
anonymity	گمنامی	غیرقابل‌تشخیص بودن از سایر هستارها در یک ویژگی مشخص
anonymization syn.: data anonymization	گمنام‌سازی مت. گمنام‌سازی داده‌ها	فرایند تغییر داده‌ها، برای اطمینان از حفظ حریم آنها، با رمزگذاری، حذف، جایگزینی، تحریف، تعمیم یا تجمیع شناسانه‌های داده‌ها
anonymizer	گمنام‌ساز	ابزاری که ردگیری فعالیت‌ها را در اینترنت ناممکن می‌سازد
arbiter physical unclonable function abbr. arbiter PUF	تابع فیزیکی تکثیرناپذیر انتخاب‌گر اختصار: 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	روشی 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 با تولید امضای دیجیتالی) 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 به‌دلیل وابستگی امنیت به رفتار طرح برای مقادیری از پارامتر امنیتی است که به اندازهٔ کافی، متناظر با طول کلید، بزرگ باشند
atomicity syn. atomicity property	تفکیک‌ناپذیری مت. ویژگی تفکیک‌ناپذیری	یکی از ویژگی‌های پرداخت‌های الکترونیکی که به کاربر امکان می‌دهد چند عمل را به‌صورت منطقی به یکدیگر چنان مرتبط سازد که یا همهٔ آن عملیات اجرا شود یا هیچ‌یک از آنها اجرا نشود

واژه بیگانه	معادل فارسی	تعریف
atomicity property syn. atomicity	ویژگی تفکیک‌ناپذیری مت. تفکیک‌ناپذیری	.

یکی از ویژگی‌های پرداخت‌های الکترونیکی که به کاربر امکان می‌دهد چند عمل را به‌صورت منطقی به یکدیگر چنان مرتبط سازد که یا همهٔ 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

attribute-based authorization — مجازشناسی ویژگی‌بنیاد

فرایندی ساختاریافته که برمبنای ویژگی‌های کاربران و داده‌ها و سامانه‌ها و خدمات، چگونگی دسترسی 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 وارسی ویژگی‌های منتسب به یک هویت

attributes management — مدیریت ویژگی‌ها

زیرمجموعهٔ مدیریت داده‌های مجازشناسی (authorization data management) که بر مبنای آن ویژگی‌ها متناظر با هستارهای موجود در یک محیط هستند

audio steganography — نهان‌نگاری صوتی

جا دادن پیام محرمانه در نشانک‌های صوتی رقمی

واژه بیگانه	معادل فارسی	تعریف
auditability	ممیزی‌پذیری	امکان بازدید مستقیم از فعالیت‌های یک سامانه برای پایش سامانه و تشخیص تخطی‌های امنیتی به‌منظور ارائهٔ پیشنهاد در اصلاح نظارت‌ها و روندها و سیاست‌ها
authenticated encryption abbr. AE	رمزگذاری احرازاصالت‌شده مت. رمزگذاری اصالت‌سنجی‌شده	راهکاری جدید برای تأمین همزمان محرمانگی و احراز اصالت که در مقایسه با راهکار قدیم، که حاصل ترکیب مستقیم روش‌های رمزگذاری و احراز اصالت بود، سرعت و کارائی بیشتری دارد
authenticated encryption with associated data abbr. AEAD	رمزگذاری احرازاصالت‌شده با داده‌های همراه مت. رمزگذاری اصالت‌سنجی‌شده با داده‌های همراه	نوعی طرح رمزگذاری احرازاصالت‌شده که در آن داده‌های کمکی، بدون رمزگذاری، احراز اصالت می‌شوند
authenticated key exchange	تبادل کلید احراز اصالت‌شده مت. تبادل کلید اصالت‌سنجی‌شده	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 وارسی 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 ارائهٔ سازوکارهای احراز اصالت فراهم می‌کند
authentication mode	شیوهٔ احراز اصالت مت. شیوهٔ اصالت‌سنجی	روشی برای به کارگیری رمز قالبی که به اطمینان از اصالت و یکپارچگی داده‌ها منجر می‌شود

واژه بیگانه	معادل فارسی	تعریف
authentication period	دورهٔ احراز اصالت مت. دورهٔ اصالت‌سنجی	بیشینه‌زمان قابل قبول بین فرایند احراز اصالت اولیه و فرایندهای احراز اصالت بعدی، در مدت زمان یک نشست واحد یا در طی زمانی که دسترسی به داده‌ها امکان‌پذیر است
authentication provider	نشان‌بخش اصالت	نهادی که مسئولیت احراز اصالت اولیهٔ هستارها را برعهده دارد و نمودافزاری به نشانهٔ احراز اصالت اولیه، به هر هستار تخصیص می‌دهد
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
authenticity	اصالت	اصیل بودن و برخورداری از قابلیت وارسی‌پذیری و اعتماد که نتیجهٔ آن اطمینان از درستی یک پیام و مبدأ پیام و انتقال آن است
authorization syn.: authorize processing security authorization	مجازشناسی مت. فرایند مجازشناسی مجازشناسی امنیت	تصمیمی مدیریتی و رسمی از سوی یک مدیر ارشد سازمان، برای مجاز کردن عملیات یک سامانهٔ اطلاعاتی و پذیرش صریح مخاطرات آن، درمورد عملیات و دارایی‌های سازمان یا افراد، براساس مجموعه‌ای از واپایش‌های امنیتی توافق‌شده
authorization algebra	جبر مجازشناسی	مجموعه‌ای از قواعد و روال‌های مورد استفاده در زیرساخت‌های ساده‌شدهٔ کلید عمومی که امکان صدور مجوز و واپایش دسترسی را فراهم می‌سازند

واژه بیگانه	معادل فارسی	تعریف
authorization architecture	معماری مجازشناسی	
		مجموعه‌ای از مؤلفه‌ها و داده‌ها که اخذ و اجرای تصمیم‌های مجازشناسی را ممکن می‌سازد
authorization boundary	محدودهٔ مجازشناسی	
		همهٔ مؤلفه‌های یک سامانهٔ اطلاعاتی که یک مقام مجازشناسی می‌تواند آنها را مجاز سازد، بی‌آن‌که شامل سایر سامانه‌های مجاز متصل به آن شود
authorization management	مدیریت مجازشناسی	
		مدیریت تخصیص مجوز به افراد یا هستارها برای انجام یک کار یا ادارهٔ یک سازمان مشخص
authorization policy	خط‌مشی مجازشناسی	
		خط مشی‌ای مرتبط با داده‌های مجازشناسی برای اتخاذ تصمیم‌های مجازشناسی که توسط مرجع تصمیم‌گیری ارائه می‌شود
authorizer	مجازشناس	
		هستاری که خط‌مشی مرجع مجازشناسی را تعیین می‌کند
authorizing official syn. accreditation authority	مقام مجازشناسی	
		مأموری رسمی با اختیارات قانونی، برای تعیین سطح پذیرفتنی از مخاطراتی که ممکن است متوجه سرمایه یا کارکنان یا عملیات در یک سامانهٔ اطلاعاتی باشد
auto-key	خودکلید	
		نوعی کلید که با استفاده از متن اصلی به دست می‌آید
auto-key cipher	رمز خودکلید	
		رمزی که در آن از متن اصلی یا دنبالهٔ کلید اجرایی برای تولید کلید استفاده می‌کنند
avalanche criterion	معیار بهمنی	
		معیاری برای ارزیابی رمزهای قالبی که براساس آن لازم است با تغییر یک بیت ورودی به خوارزمی/الگوریتم رمز به‌طور متوسط نیمی از بیت‌های خروجی آن تغییر کند

واژه بیگانه	معادل فارسی	تعریف
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 پس‌سو	

خصوصیتی که بنا بر آن لو رفتن کلید نشست‌های پیشین باعث نمی‌شود که امنیت نشست کنونی به خطر بیفتد

balance property	ویژگی توازن	

برابری شمار صفرها و یک‌ها در یک دورهٔ تناوب از یک دنبالهٔ دودویی متناهی به طول بیشینه

band scrambler syn.: band splitter	درهم‌ریز باند مت. جداساز باند	

ابزاری برای تقسیم طیف بسامدی به تعدادی زیرباندهای مساوی و درهم ریختن نشانک/سیگنال از طریق بازچینش ترتیب آن‌ها

bi-deniable encryption	رمزگذاری دوسوانکارپذیر	

نوعی رمزگذاری 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 (نویسه‌ها) در متن رمز

bilinear Diffie-Hellman problem abbr. BHD problem	مسئلهٔ دیفی ـ هلمن دوخطی	

مسئله محاسبهٔ $\hat{e}\ (p,p)^{abc}$ با در اختیار داشتن چهارتایی (p, ap, bp, cp) و با این فرض که G_2 و G_1 دو گروه دوری از مرتبهٔ عدد اول q و $\hat{e}$ یک نگاشت دو خطی از $G_1 \times G_1$ به G_2 و p مولدی برای G_1 باشد

binding	ترابست	

۱. فرایند ایجاد تناظر بین دو عنصر اطلاعاتی مرتبط
۲. تأیید ارتباط شناسهٔ یک هستار با کلید عمومی آن توسط یک نهاد مورد اعتماد

واژه بیگانه	معادل فارسی	تعریف
biometric concealer attack	حملهٔ پنهان‌ساز زیست‌سنجشی	نوعی حمله که در آن حمله‌کننده، چه به‌وسیلهٔ یک دست‌ساخته و چه از طریق پوشش یا تغییر مشخصه‌های زیستی طبیعی، قصد پنهان کردن مشخصه‌های زیستی را دارد
biometric impostor attack	حملهٔ فریب‌دهندهٔ زیست‌سنجشی	نوعی حملهٔ وانمودسازی که در آن حمله‌کننده می‌خواهد به جای فرد دیگری شناسایی شود
bipartite substitution syn. digraphic substitution	جانشینی دوبخشی	نوعی جانشینی که در آن از دونگاشت‌ها برای جایگزینی دونویسه‌ها(زوج‌های مرتب از نویسه‌ها)ی متن اصلی استفاده می‌شود
birthday attack	حملهٔ 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 دست‌کم 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 abbr. BIC	معیار استقلال بیتی	معیاری که به‌موجب آن، تغییر هر بیت ورودی در توابع بولی به تغییر هر دو بیت خروجی دلخواه، به‌طور مستقل از یکدیگر، منجر می‌شود

واژه بیگانه	معادل فارسی	تعریف
Byzantine fault	خطای بیزانسی	وضعیتی در یک سامانهٔ محاسباتی توزیع‌شده که در آن ممکن است برخی مؤلفه‌ها از کار بیفتند درحالی‌که اطلاعات کاملی برای تعیین ازکارافتادگی مؤلفه(ها) و شناسایی مؤلفه(ها)ی ازکارافتاده وجود نداشته باشد
Byzantine fault tolerance abbr. BFT	تاب‌آوری خطای بیزانسی اختصار: تاخاب	توانایی یک سامانهٔ محاسباتی برای مواجهه با داده‌های مشکوک ناشی از خطای بیزانسی
Byzantine General's Problem	مسئلهٔ سرداران بیزانسی	مسئلهٔ دستیابی به اجماع، توسط تعدادی نهاد غیرمتمرکز، بدون استفاده از یک نهاد مرکزی قابل‌اعتماد
blind proxy signature	امضای وکالتی کور	امضایی که در آن امضاکنندهٔ اصلی نمی‌تواند امضاکنندهٔ 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	ته‌نقش‌گذاری کور	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 درخدمات‌رسانی که در آن ارائه‌دهندهٔ خدمات از درونداد یا برونداد واقعی بی‌خبر است
block	ریسهٔ یک	یک‌های متوالی در یک دنبالهٔ دودویی که بیت پیش و پس از آن صفر باشد

واژه بیگانه	معادل فارسی	تعریف
black hole attack syn.: packet drop attack	حملهٔ سیاه‌چاله‌ای مت. حملهٔ از دست رفتن بسته	نوعی حملهٔ بندآوری خدمات که در آن یک گره بدخواه، با این ادعای نادرست که یک مسیر تازه برای رسیدن به مقصد دارد، تمام بسته‌ها را بدون انتقال به مقصد به سمت خود می‌کشد و در خود جذب می‌کند
boomerang attack	حملهٔ بومرنگی	نوعی حملهٔ آماری-ساختاری که در دو گام اصلی انجام می‌شود؛ در گام اول با پیچیدگی پایین‌تر از جستجوی فراگیر، دنبالهٔ خروجی سامانهٔ رمز از یک دنبالهٔ تصادفی متمایز می‌شود و در گام دوم بیت‌های کلید سامانهٔ رمز، با استفاده از مشخصه‌های متمایزکنندهٔ گام اول، بازیابی می‌شوند
branch number	عدد انشعاب	عددی که به‌عنوان معیاری برای سنجش قدرت پخش یک نگاشت به کار می‌رود
broadcast encryption	رمزگذاری پخش	روشی مؤثر برای پخش اطلاعات در میان یک گروه درحال‌تغییر، به‌صورتی‌که فقط افراد دارای مجوز دریافت اطلاعات، امکان رمزگشایی آن را داشته باشند
brute force attack syn. exhaustive key search	حملهٔ 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
central ledger syn. centralized ledger,general ledger	دفترکل مرکزی مت.: دفترکل عمومی	مخزن اصلی یکتایی که سوابق تراکنش‌های یک هستار تجاری در آن نگهداری می‌شود و معمولاً واپایش آن را شخص واحد یا گروهی محدود از افراد برعهده دارند

واژه بیگانه	معادل فارسی	تعریف
certificate authority syn. certification authority abbr. CA	مرجع صدور گواهی	نهادی رسمی و معتبر که وظیفهٔ صدور و مدیریت و انتشار و فسخ گواهینامه‌های کلید عمومی را بر عهده دارد
certificate revocation list	فهرست ابطال گواهی	فهرستی از گواهی‌های کلید عمومی که مرجع صدور گواهی، پیش از انقضا، از اعتبار ساقط کرده است
certification	صدور گواهی	روند صدور گواهی برای تأیید هر هستار
certification authority syn. certificate authority abbr. CA	مرجع صدور گواهی	نهادی رسمی و معتبر که وظیفهٔ صدور و مدیریت و انتشار و فسخ گواهینامه‌های کلید عمومی را بر عهده دارد
certification policy abbr. CP	خط‌مشی گواهی	سیاست حاکم بر همهٔ مراحل مربوط به تولید و توزیع و حسابرسی و ابطال گواهی‌های رقمی
certification practice statement	شیوه‌نامهٔ صدور گواهی	بیانیه‌ای که در مدیریت گواهی‌ها بر پایهٔ آن عمل می‌شود
challenge-response authentication	اصالت‌سنجی چالش‌پاسخی	نوعی قرارداد احراز اصالت که در آن، در طی فرایند پرسش‌وپاسخ، هویت یک هستار احراز می‌شود
challenge-response identification	شناسایی چالش‌پاسخی	نوعی قرارداد شناسایی که در آن در طی فرایند پرسش‌وپاسخ یک هستار شناسایی می‌شود
cheater	فریب‌دهنده	یکی از طرف‌های قرارداد، که در حین اجرای قرارداد دروغ می‌گوید یا از آن قرارداد پیروی نمی‌کند

واژه بیگانه	معادل فارسی	تعریف
chosen ciphertext attack	حمله با متن رمز منتخب	حمله‌ای (تحلیل رمزی) که در آن مهاجم قادر به انتخاب متن‌های رمز و مشاهدهٔ متن‌های اصلی متناظر با آن است
chosen message attack	حملهٔ پیام‌منتخب	نوعی تهاجم به‌صورت جعل امضا که براساس ارسال شماری پیام منتخب از سوی مهاجم و اقناع امضاکننده به امضای آنها انجام می‌شود
chosen plaintext attack	حمله با متن اصلی منتخب	حمله‌ای (تحلیل رمزی) که در آن مهاجم توانایی انتخاب متن‌های ساده و مشاهده یا دریافت متن‌های رمزی‌شدهٔ متناظر را دارد
chosen related key attack	حملهٔ کلیدمرتبط منتخب	حمله‌ای به فرانمای کلید که در آن مهاجم با انتخاب رابطهٔ بین چند کلید و دسترسی به توابع رمزگذاری متناظر در پی یافتن کلید است
chosen-key attack	حملهٔ کلیدمنتخب	دسته‌ای از حمله‌ها که در آن مهاجم تنها با اطلاع از وجود رابطه‌ای بین کلیدهای مختلف و کاهش فضای جست و جو، سعی در دستیابی به کلید دارد
chosen-text attack	حملهٔ متن‌منتخب	حمله‌هایی مرکب از حمله‌های با متن اصلی منتخب و با متن اصلی منتخب وفقی و با متن رمز منتخب
cipher syn. encryption algorithm	رمز مت. الگوریتم/خوارزمی رمزگذاری	خوارزمی/ الگوریتمی برای تبدیل متن اصلی به متن رمزی‌شده به‌نحوی‌که برای گیرندهٔ غیرمجاز غیرقابل‌درک باشد
cipher feedback mode	شیوهٔ بازخورد رمز	یکی از روش‌های به‌کارگیری رمز قالبی که در آن از متن رمز تولیدشده در یک مرحله از رمزگذاری، برای تولید متن رمز متناظر با متن اصلی بعدی استفاده می‌شود

واژه بیگانه	معادل فارسی	تعریف
cipher system syn. cryptosystem syn. cryptographic system	سامانه رمز مت. سامانه رمزنگاشتی	

سامانه‌ای متشکل از خوارزمی‌ها/ الگوریتم‌های رمزگذاری و رمزگشایی همراه با مجموعهٔ سه‌گانهٔ متن‌های اصلی و متن‌های رمزی‌شده و کلیدها

ciphertext/ cipher text syn. cryptogram	متن رمزی‌شده مت. متن رمز، رمزنگاشت

خروجی الگوریتم رمزگذاری، داده ی رمز شده

cipher text auto-key	خودکلید متن رمز

منطق رمزنگاشتی که در آن از متن رمزشدهٔ قبلی برای تولید یک دنبالهٔ کلید اجرایی استفاده می کنند

ciphertext-ciphertext compromise	مخاطرهٔ کلید متن‌رمز ـ متن‌رمز

لو رفتن اطلاعات کلید که از تحلیل اطلاعات حاصل از رمزگذاری یک متن اصلی با دو کلید متفاوت حاصل می‌شود.

ciphertext-only attack	حملهٔ فقط با متن رمز

حمله‌ای که در آن تحلیلگر رمز به متن رمزی‌شدهٔ شماری از پیام‌هایی دسترسی دارد که همگی با یک خوارزمی/ الگوریتم، رمزگذاری (encryption) شده‌اند

ciphony 1	رمزآوا

اطلاعات صوتی رمزگذاری‌شده

ciphony 2	رمزآوایی

فرایند رمزگذاری اطلاعات صوتی

clear text/ cleartext syn. plaintext	متن آشکار مت. متن ساده

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

واژه بیگانه	معادل فارسی	تعریف
clock-controlled generator	مولد ساعت‌فرما	
مولدی برای تولید دنباله‌های دودویی که براساس سازوکار ساعت عمل می‌کند		
code-based cryptography	رمزنگاری کدبنیاد	
نوعی سامانهٔ رمز پساکوانتومی که در آن اولیهٔ رمزنگاشتی (تابع یک‌طرفهٔ مبنا) از یک کد تصحیح خطای C استفاده می‌کند؛ این اولیه ممکن است شامل اضافه کردن یک خطا به کلمهٔ کد یا محاسبهٔ یک نشانگان مرتبط با ماتریس توازن‌آزمای (parity check matrix) کد باشد		
codebook	کدنامه	
مجموعه‌ای از زوج‌متن‌های اصلی و رمز متناظر با آن‌ها که با استفاده از یک کلید ثابت مشترک بدست آمده‌اند		
codebook attack	حملهٔ کدنامه	
نوعی حملهٔ متن اصلی معلوم که در آن حمله‌کننده به یک مجموعه از زوج‌متن‌های اصلی و رمز متناظر با آنها (کدنامه) دسترسی دارد و بدون دانستن کلید مخفی از آنها برای رمزگشایی پاره‌ای از ارتباطات بعدی کمک می‌گیرد		
cold storage	انبارهٔ سرد	
افزاره‌ای الکترونیکی که می‌تواند ارزهای رقمی/ دیجیتال را بدون نیاز به اتصال برخط به اینترنت ذخیره کند و احتمال دسترسی غیرمجاز و حملات رخنه‌گری (hacking attacks) و سایر آسیب‌پذیری‌هایی را که یک سامانهٔ برخط مستعد آن است کاهش دهد		
cold wallet	کیف‌پول سرد	
نوعی کیف پول رقمی/ دیجیتالی که در آن از فنّاوری انبارش سرد استفاده می‌کنند		
collision attack	حملهٔ برخوردی	
نوعی حمله برای یافتن مقادیر متمایز ورودی به یک تابع که دارای خروجی یکسان باشند.		
collision free hash function	تابع چکیده‌ساز بی‌برخورد	
نوعی تابع چکیده‌ساز یک‌طرفه که در آن دو پیام ورودی متفاوت، ازنظر محاسباتی، خروجی یکسان نداشته باشد		

واژه بیگانه	معادل فارسی	تعریف
collision resistance	برخوردتابی	عدم امکان یافتن دو ورودی با خروجی یکسان برای یک تابع چکیده‌ساز ازنظر محاسباتی
commitment scheme	طرح تعهد	قراردادی که براساس آن یکی از طرف‌ها (فرستنده) می‌تواند در برابر طرف مقابل (گیرنده) نسبت به مقداری مانند x متعهد شود به‌گونه‌ای که بعداً قادر به افشای آن باشد، ولی تا آن لحظه این مقدار برای گیرنده پوشیده باقی می‌ماند و پس از افشا، گیرنده می‌تواند درستی مقدار افشاشده و برابری آن را با مقداری که نسبت به آن تعهد داده شده وارسی کند
communications cover	پوشش ارتباطاتی	پنهان‌سازی یا تغییر مشخصات الگوهای ارتباطات برای مخفی کردن اطلاعاتی که می‌تواند برای رقیب یا دشمن ارزشمند باشد
communications deception	فریب ارتباطاتی	ارسال یا بازارسال یا تغییر آگاهانهٔ ارتباطات با هدف گمراه‌سازی دشمن
communications profile	رخ‌نمای ارتباطات	الگویی تحلیلی از ارتباطات وابسته به یک سازمان یا فعالیت که از آزمون نظام‌مند محتوا و الگوهای ارتباطات و توابع حاصل از آنها و سنجش‌های کاربردی امنیت ارتباطات حاصل می‌شود
communications security abbr. COMSEC	امنیت ارتباطات	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

واژه بیگانه	معادل فارسی	تعریف
complexity theory	نظریهٔ پیچیدگی	نظریه‌ای برای تعیین منابع لازم برای حل مسائل خوارزمیک/ الگوریتمی و درنتیجه تعیین این که چه مسائلی با منابع دسترس‌پذیر حل‌پذیرند
compromise	به‌خطرافتادگی کلید	افشا یا تغییر یا جایگزینی یا استفادهٔ غیرمجاز از داده‌های حساس از جمله کلیدهای رمزنگاشتی (cryptographic keys) و دیگر پارامترهای امنیتی خطیر
compromised key	کلید به‌خطرافتاده	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 نظریهٔ اعداد و خوارزمی‌ها/ الگوریتم‌های محاسباتی
computational complexity theory	نظریهٔ پیچیدگی محاسباتی	مطالعهٔ کمینه منابع مورد نیاز برای حل مسائل محاسباتی
computational security	امنیت محاسباتی	امنیت کمّی در مقابل رمزگشایی غیرمجاز بر پایهٔ فرضیات خاصی که تحلیلگر در مورد رمز در نظر می‌گیرد
computationally secure steganography	نهان‌نگاری محاسباتی‌امن	نوعی خوارزمی/ الگوریتم نهان‌نگاری که مهاجم با در اختیار داشتن یک خوارزمی/ الگوریتم محاسباتی زمان‌چندجمله‌ای (polynomial-time computable algorithm) احتمالاتی تنها بتواند تمایز ناچیزی بین پوشانه و نهانه پیدا کند

واژه بیگانه	معادل فارسی	تعریف
computer incident response center abbr. CIRT syn. computer incident response team abbr. CIRC syn. cyber incident response team	مرکز رویارویی با پیشامدهای رایانه‌ای اختصار: مرکز روپر مت. گروه رویارویی با پیشامدهای رایانه‌ای اختصار: گروه روپر	گروهی از تحلیل‌گران امنیت رایانه که به‌منظور مهار و ریشه‌کنی پیشامدهای امنیتی در رایانه ها و بازیابی آسیب‌های ناشی از آنها گردهم آمده باشند
COMSEC (communications security) material control system abbr. CMCS	سامانهٔ واپایی اجزای امنیت ارتباطات (سوار)	سامانهٔ تدارکاتی و حسابداری که از طریق آن اجزای امنیت ارتباطات با برچسب «رمز» (CRYPTO) توزیع و واپایش و حراست می‌شوند
concurrent setting	تنظیم هم‌رو	تنظیمی برای تحلیل طرح‌های اثبات ناتراوا که در آن چندین وارسی‌کننده، احتمالاً بدخواه، در برابر یک اثبات‌کننده در نظر گرفته می‌شوند؛ وارسی‌کنندگان در اجراهای مستقل با اثبات‌کننده تعامل دارند و با انجام یک حملهٔ هماهنگ مشترک سعی می‌کنند اطلاعاتی غیربدیهی را از اثبات‌کننده به چنگ آورند
concurrent zero-knowledge proof	اثبات ناتراوای هم‌رو مت. اثبات دانش‌صفر هم‌رو	نوعی اثبات ناتراوا که حتی در صورت اجرای نسخه‌های پرشماری از آن در یک محیط ناهم‌زمان، مانند اینترنت، باز هم ناتراوا باقی بماند
confirmer signature syn:designated confirmer signature	امضای تائیدیار مت. امضای تأییدیارمشخص	نوعی امضا که بدون کمک امضاکننده یا یک شخص ثالث نیم‌معتمد قابل وارسی نیست
controlled cryptographic item abbr. CCI	رمزاقلام واپاییده اختصار: راوا	سامانهٔ اطلاعاتی یا مخابراتی امن یا مؤلفهٔ رمزنگاشتی مرتبط با آن سامانه که بدون طبقه‌بندی است و به‌وسیلهٔ سامانهٔ واپایی اجزای امنیت ارتباطات (سوار)، یک سامانهٔ واپایی کلی معادل یا ترکیبی از هر دو راهبری می‌شود و پاسخ‌گویی و رؤیت‌پذیری را فراهم می‌کند

واژه بیگانه	معادل فارسی	تعریف
controlled cryptographic item assembly abbr. CCI assembly	هم‌گذاری رمزاقلام واپاییده اختصار: هم‌گذاری راو	

دستگاهی حاوی یک منطق رمزنگاشتی یا یک طرح امنیت ارتباطاتی دیگر که موردتأیید آژانس امنیت ملی امریکا (NSA) به‌عنوان یک مؤلفهٔ رمزاقلام واپاییده (مؤلفهٔ راوا) باشد؛ این دستگاه کل عملیات امنیت ارتباطات را اجرا می‌کند ولی برای این کار به تجهیزات میزبان وابسته است

controlled cryptographic item component abbr. CCI component	مؤلفهٔ رمزاقلام واپاییده اختصار: مؤلفهٔ راوا	

قسمتی از اقلام رمزنگاشتی واپاییده که به تجهیزات میزبان یا همایه برای کامل‌کردن و اجرای کار امنیت ارتباطات وابسته است اما کل کار امنیت ارتباطات را انجام نمی‌دهد

controlled cryptographic item equipment abbr. CCI equipment	تجهیزات رمزاقلام واپاییده اختصار: تجهیزات راوا	

تجهیزات راهبری مخابرات یا اطلاعات که حاوی مؤلفه‌ای از اقلام رمزنگاشتی واپاییده یا همایهٔ اقلام رمزنگاشتی واپاییده است و کل کار امنیت ارتباطات را بدون وابستگی به تجهیزات میزبان انجام می‌دهد

correlation attack	حملهٔ همبستگی	

نوعی حملهٔ مبتنی بر روش تقسیم‌وحل که از وابستگی آماری میان دنبالهٔ کلید اجرایی و خروجی یکی از ثاب‌های خطی سازندهٔ رمز جریانی برای یافتن حالت اولیهٔ همان ثاب خطی استفاده می‌کند

correlation immunity	ایمنی از همبستگی	

در توابع بولی، ویژگی یک تابع بولی n متغیرهٔ f، هرگاه اطلاعات متقابل بین خروجی و همهٔ زیربُردارهای k تایی از متغیرهای ورودی صفر باشد

counter mode syn. integer counter mode	شیوهٔ شمارگر مت. شیوهٔ شمارگر صحیح	

یکی از روش‌های معیار به‌کارگیری رمز قالبی (block cipher) که در آن ابتدا دنباله‌ای از اعداد به‌عنوان ورودی خوارزمی/ الگوریتم رمز وارد می‌شود، سپس قالب‌های متن اصلی به‌ترتیب با قالب‌های خروجی خوارزمی /الگوریتم رمز ترکیب می‌شوند تا متن رمزشدهٔ متناظر با هر قالب به دست آید؛ پس از رمزگذاری هر قالب به مقدار شمارگر، مقدار ثابتی، معمولاً یک واحد، افزوده می‌شود

واژه بیگانه	معادل فارسی	تعریف
covertext	پوشانه	پیامی که داده‌های پیام محرمانه در داخل داده‌های آن درج می‌شود
cryptanalysis	تحلیل رمز	1. بررسی امنیت سامانه‌های رمز ازطریق جست‌وجوی خطاها یا ضعف‌های احتمالی خوارزمی/ الگوریتم آنها به قصد ممانعت از نفوذ مهاجم و بالا بردن ضریب امنیت سامانه 2. عملیات محاسباتی برای به دست آوردن کلید سامانهٔ رمز، بدون آگاهی از کلید آن، با هدف نفوذ به سامانه
cryptanalyst	تحلیل‌گر رمز	فردی که تحلیل رمز می‌کند و در آن تخصص دارد
cryptographic primitive	نخستینهٔ رمزنگاشتی	خوارزمی‌ها/الگوریتم‌های رمزنگاشتی شناخته‌شده و سطح‌پایین، شامل توابع چکیده‌ساز یک‌طرفه و توابع رمزگذاری که به‌طورمعمول به‌منظور ساخت یا طراحی قراردادهای رمزنگاشتی برای سامانه‌های امنیت رایانه‌ای به‌کار می‌روند
cryptographic protocol	قرارداد رمزنگاشتی	یک خوارزمی/ الگوریتم توزیع‌شده که به‌طور دقیق تعامل میان دو یا چند هستار را برای دسترسی به اهداف امنیتی مشخص بیان می‌کند
crypto machine	ماشین رمز	ماشین‌هایی قدیمی برای رمزگذاری خودکار، با استفاده از ترکیب انواعی از جانشینی‌های الفبایی، که اغلب با استفاده از چرخانه عمل می‌کنند
crypto officer	کارشناس رمز، مسئول رمز	فرد یا اداره‌ای برای اجرای امور رمزنگاشتی کارور یا فرایندی برای آماده‌سازی اولیه یا مدیریتی رمزنگاشتی
crypto period syn. key lifetime	رمزدوره مت. طول عمر کلید	بازه‌ای زمانی که در آن کلید رمزگذاری برای یک سامانهٔ رمز معتبر است

واژه بیگانه	معادل فارسی	تعریف
cryptocurrency	رمزارز	

نوعی ارز که تنها به صورت رقمی وجود دارد و فرایندهای تولید، وارسی و انتقال آن با استفاده از روش‌های رمزنگاشتی و مستقل از یک بانک مرکزی، تنظیم می شود

cryptogram syn. ciphertext	متن رمز، رمزنگاشت مت. متن رمزی‌شده	

خروجی الگوریتم رمزگذاری، یا داده ی رمز شده

cryptographic	رمزنگاشتی	

مربوط به رمزنگاری یا به شیوهٔ رمزنگاری

cryptographic alarm	آژیر رمزنگاشتی	

مدار یا افزاره‌ای که خرابی‌ها یا انحراف را در منطق یا عملکرد تجهیزات رمز تشخیص می‌دهد و ممکن است یا مانع از ارسال پیام شود یا هشدار دیداری یا شنیداری تولید کند

cryptographic algorithm	الگوریتم رمزنگاشتی مت. خوارزمی رمزنگاشتی	

یک روال محاسباتی که بر مبنای تعدادی متغیر ورودی، شامل یک کلید رمزنگاشتی، خروجی را تولید می‌کند

cryptographic hash function syn. hash function syn. hashing algorithm	تابع چکیده‌ساز رمزنگاشتی مت. تابع چکیده‌ساز مت. خوارزمی/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 برخوردتابی است

cryptographic mode	شیوهٔ رمزنگاشتی	

شیوه‌ای برای تأمین امنیت که در آن خوارزمی/ الگوریتم‌های رمز پایه و انواعی از بازخوردها و عملگرهای ساده به گونه‌ای ترکیب می‌شوند که امنیت مجموعهٔ حاصل، تابعی از امنیت الگوریتم/خوارزمی رمز به‌کاررفته باشد

واژه بیگانه	معادل فارسی	تعریف
cryptographic module	پودمان رمزنگاشتی	

مجموعهٔ سخت‌افزار و نرم‌افزار و ثابت‌افزار برای اجرای توابع امنیتی تأییدشده شامل خوارزمی/ الگوریتم‌های رمزنگاشتی و تولید کلید

cryptographic module security policy	خط‌مشی امنیتی پودمان رمزنگاشتی

خط مشی‌ای منطبق بر قواعد دقیق امنیتی که یک واحد رمزنگاشتی تحت آن عمل می‌کند

cryptographic coprocessor syn.cryptoprocessor/crypto-processor	همپرداز رمزنگاشتی مت.رمزپرداز

واحدی سخت‌افزاری شامل یک پردازندهٔ خاص برای عملیات رمزنگاشتی و پردازش‌های مرتبط

cryptographic scheme	طرح رمزنگاشتی

مجموعه‌ای از خوارزمی/ الگوریتم‌ها و قراردادهای رمزنگاشتی مرتبط برای دستیابی به اهداف امنیتی مشخص

cryptographic security	امنیت رمزنگاشتی

یکی از مؤلفه‌های امنیت ارتباطات، حاصل از تامین و استفاده فنیِ صحیح از سامانه‌های رمزنگاشتی مناسب

cryptographic strength	استحکام رمزنگاشتی

معیاری مبتنی بر تعداد عملیات مورد انتظار که برای شکستن یک سازوکار رمزنگاشتی نیاز است

cryptographic system syn. cipher system syn. cryptosystem	سامانه رمزنگاشتی مت. سامانه رمز

سامانه‌ای متشکل از خوارزمی‌ها/ الگوریتم‌های رمزگذاری و رمزگشایی همراه با مجموعهٔ سه‌گانهٔ متن‌های اصلی و متن‌های رمزی‌شده و کلیدها

cryptologist	رمزشناس

متخصص علم رمزشناسی

واژه بیگانه	معادل فارسی	تعریف
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 پردازندهٔ 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 مجموعهٔ سه‌گانهٔ متن‌های اصلی و متن‌های رمزی‌شده و کلیدها

cube attack	حملهٔ مکعبی	

حمله‌ای که در آن از سازوکاری خاص برای حل سامانهٔ حاصل از معادلات چندجمله‌ای، برحسب متغیرهای سرّی مشترک آنها، استفاده می‌شود؛ تقریباً تمام طرح‌های رمزنگاشتی را می‌توان به‌صورت یک چندجمله‌ای تنظیم‌پذیر چندمتغیره $p(x_1, \ldots, x_n, v_1, \ldots, v_m)$، روی $GF(2)$ متشکل از متغیرهای سرّی x_i (بیت‌های کلید و مقادیر اولیه) و متغیرهای عمومی v_i (بیت های متن اصلی)، توصیف کرد. در این حمله مهاجم می‌تواند به‌طور آزادانه متغیرهای عمومی، یا متغیرهای قابل‌تنظیم خاصی را در چندجمله‌ای اصلی مقداردهی کند

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 ریشه‌کنی پیشامدهای امنیتی در رایانه ها و بازیابی آسیب‌های ناشی از آنها گردهم آمده باشند

D

data complexity	پیچیدگی داده‌ای	

میزان دادهٔ مورد نیاز برای انجام یک حمله

واژه بیگانه	معادل فارسی	تعریف
data encapsulation mechanism abbr. DEM	سازوکار لفاف‌بندی داده اختصار: سِلد	محافظت از رازمانی و یکپارچگی انبوه داده‌ها به روش‌های متقارن
data encryption	رمزگذاری داده‌ها	فرایندی که در آن داده‌ها به دلایل امنیتی رمزگذاری شوند
data encryption standard abbr. DES	استاندارد رمزگذاری داده‌ها	خوارزمی/ الگوریتم مورد توافق (استاندارد) برای رمزگذاری یا رمزگشایی داده‌ها با استفاده از جدول رمز ۶۴ بیتی
data scrambler	درهم‌ریز داده	ابزاری برای مبهم‌سازی داده‌ها، با استفاده از صافی‌های پی‌درپی خطی با پسخوردها، شمارنده‌ها، انباره‌ها و مدارهای منطقی جانبی
data security	امنیت داده	حفاظت از داده‌ها در مقابل تغییر غیرمجاز عمدی یا تصادفی، تخریب یا افشای آن ها
deanonymization	گمنامی‌زدایی	وارون فرایند گمنام‌سازی، به‌گونه‌ای که با تغییر داده‌ها آن‌ها را قابل شناسایی می‌کنند
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 رمزشده به متن اصلی متناظر با استفاده از خوارزمی/الگوریتم خاص آن
decision problem	مسئلهٔ تصمیم	تصمیم‌گیری دربارهٔ این که آیا رشتهٔ ورودی برخی از ویژگی‌های مشخص‌شده را برآورده می‌کند یا خیر

واژه بیگانه	معادل فارسی	تعریف
decisional Diffie-Hellman problem	مسئلهٔ تصمیم دیفی ـ هلمن	مسئلهٔ اخذ تصمیم در مورد برقراری رابطهٔ $c = ab\ (mod\ q)$ براساس 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	رمزگشایی‌شده	اطلاعات یا داده‌های رمزگذاری‌شده‌ای که به اطلاعات یا داده‌های آشکار تبدیل شده باشند
decrypting syn. deciphering	رمزگشایی	فرآیند تبدیل اطلاعات رمزشده به متن اصلی متناظر با استفاده از خوارزمی/الگوریتم خاص آن
decryption mixnet	شبکهٔ مخلوط رمزگشایی	نوعی شبکهٔ مخلوط که در آن ورودی‌های هر مرحله با استفاده از کلید خصوصی متناظر با آن مرحله بازگشایی می‌شوند
de-identification	شناسایی‌زدایی	فرایند حذف اطلاعات شخصی از یک پرونده یا مجموعهٔ داده برای محافظت از حریم خصوصی افراد
Diffie-Hellman key agreement	توافق کلید دیفی–هلمن	نوعی طرح توافق کلید که به دو طرف ارتباط اجازه می‌دهد با مبادلهٔ مقادیر عمومی و استفاده از این مقادیر و مقادیر خصوصی متناظر، یک کلید مشترک را به‌طور امن محاسبه کنند
delay-based silicon PUF	تابع فیزیکی تکثیرناپذیر سیلیکونی (سیلیسیمی) تأخیرمبنا / تفت سیلیکونی(سیلیسیمی) تأخیرمبنا	دسته‌ای از توابع فیزیکی تکثیرناپذیر سیلیکونی که خروجی آن‌ها از طریق اندازه‌گیری متغیرهای تصادفی حاصل از تأخیر یک مدار رقمی/دیجیتالی به‌دست می‌آید

واژه بیگانه	معادل فارسی	تعریف
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 به‌نحوی که گیرنده نتواند شخص سومی را متقاعد کند که چنین احراز اصالتی یا هر احراز اصالتی تا کنون انجام شده‌است

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	

کلیدی که توسط یک خوارزمی/ الگوریتم مشخص محاسبه می‌شود که ورودی آن شامل داده‌های عمومی و محرمانه است

designated confirmer signature syn: confirmer signature	امضای تأییدیارمشخص مت. امضای تأییدیار	

نوعی امضا که بدون کمک امضاکننده یا یک شخص ثالث نیم‌معتمد قابل وارسی نیست

designated-verifier signature	امضای وارس مشخص	

نوعی امضای رقمی که در آن وارسی‌کنندهٔ مشخصی از اعتبار پیام امضاشده مطمئن می‌شود، اما نمی‌تواند شخص ثالث یا نهاد دیگری را قانع کند

destructive attack	حملهٔ ویرانگر	

حمله‌ای که با قصد تخریب و وارد کردن خسارات سنگین به سازمان‌های هدف طراحی و اجرا می‌شود

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

واژه بیگانه	معادل فارسی	تعریف

dictionary attack — حملهٔ واژه‌نامه‌ای

نوعی حمله برای شناسایی گذرواژه با آزمودن پی‌درپی واژه‌های واژه‌نامه‌ای که احتمال می‌رود دربردارندهٔ گذرواژه باشد

differential cryptanalysis — تحلیل تفاضلی رمز

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 تحلیل با متن اصلی منتخب با راهکار دومرحله‌ای 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
Abbr. DHP — مسئلهٔ دیفی ـ 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 می شوند

Digital Signature Standard
abr.: DSS — استاندارد امضای رقمی/ استاندارد امضای دیجیتال

استاندارد دولت فدرال ایالات متحده برای تولید امضای رقمی/ دیجیتالی که در آن از خوارزمی/ الگوریتم رمزنگاشتی کلید عمومی DSA و خوارمی/ الگوریتم چکیده‌ساز SHA-1 استفاده می‌شود

digital steganography — نهان‌نگاری رقمی

پنهان سازی اطلاعات رقمی محرمانه از طریق درج آن ها در داخل داده‌های پیام عادی

digraph
syn.: bigram — دونویسه

یک زوج مرتب متشکل از حروف (نویسه‌ها) در متن رمز

واژه بیگانه	معادل فارسی	تعریف
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

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 می‌کند

distance bounding protocol قرارداد فاصله‌محدود

قراردادی رمزنگاشتی که در آن یکی از طرف‌های ارتباط مایل است برای فاصلهٔ فیزیکی خود با طرف مقابل یک کران بالا تعیین کند

distinguishing attack حملهٔ تمایزی

حمله‌ای با هدف تفکیک جریان کلید از یک دنبالهٔ واقعاً تصادفی

distributed key generation تولید کلید توزیعی

قراردادی که به‌منظور دستیابی به اجماع در مورد یک کلید مخفی تسهیم‌شدهٔ یکبارمصرف به‌وسیلهٔ مجموعه‌ای از طرف‌های مرتبط اجرا می‌شود

distributed key management مدیریت کلید توزیعی

فرایندی رمزنگاشتی که در آن چند شرکت‌کننده، مجموعه‌ای استاندارد از کلیدهای عمومی و خصوصی را با استفاده از قراردادها(پروتکل‌ها) و خوارزمی/الگوریتم‌های اجماع خاص محاسبه می‌کنند

divide-and-conquer attack حملهٔ تقسیم و حل

نوعی حمله که در آن کلید رمز با استفاده از وجود همبستگی بین خروجی تابع ترکیب‌کنندهٔ رمز و شماری از مؤلفه‌های ورودی آن به دست می‌آید

واژه بیگانه	معادل فارسی	تعریف
dynamic adversary syn. adaptive adversary	مهاجم پویا مت. مهاجم وفقی	

مهاجمی که در طول اجرای یک پروتکل تصمیم می‌گیرد 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 به‌روزرسانی زوج‌کلیدهای اختصاصی یک یا چند عضو گروه، بدون تغییر باقی بماند

E

eavesdropper
syn. EVE — شنودگر

شخص یا نهادی که به‌صورت غیرمجاز به داده‌های یک شبکهٔ ارتباطی دسترسی می‌یابد

eavesdropping — شنود

ورود مخفیانه به یک شبکهٔ ارتباطی، اعم از صوتی یا نوشتاری، بدون ایجاد هرگونه تغییر در محتوا یا اختلال در آن

electromagnetic attack — حملهٔ الکترومغناطیسی

حمله‌ای که در آن حمله‌کننده از نشت تابش الکترومغناطیسی سامانهٔ رمز، به اطلاعات مربوط به کلید مخفی دست می‌یابد

electronic codebook mode — شیوهٔ کدنامهٔ الکترونیکی

ساده‌ترین شیوهٔ به‌کارگیری رمزهای‌های قالبی که در آن قالب‌های یکسان متن اصلی همیشه به قالب‌هایی یکسان از متن رمزشده تصویر می‌شوند و به این‌ترتیب، امکان تشکیل یک کدنامه از زوج‌های متن اصلی و رمز متناظر فراهم می‌شود

elliptic curve cryptography — رمزنگاری مبتنی بر خم بیضوی

نوعی سامانهٔ رمزنگاری کلید عمومی، مبتنی بر ساختار ریاضی خم‌های بیضوی

واژه بیگانه	معادل فارسی	تعریف
embedded system	سامانهٔ نهفته	سامانه‌ای رایانه‌ای، که بخشی از یک سامانهٔ بزرگتر است و کار خاصی را انجام می‌دهد؛ این سامانه به‌عنوان سامانهٔ بی‌درنگ نیز توصیف می‌شود؛ یعنی سامانه‌هایی که پاسخ بی‌درنگ دارند و باید مشخصه‌های مهمی از قبیل ایمنی، دسترس‌پذیری، اطمینان‌پذیری و همچنین اتکاپذیری را دارا باشند. این سامانه‌ها اغلب از دید کاربر پوشیده هستند
embedding efficiency	کارایی نهفته‌سازی	معیاری برای تعیین کیفیت اجرای خوارزمی/ الگوریتم نهفته‌سازی
encipher syn. encrypt	رمزگذاری کردن	تبدیل متن اصلی به متن رمزگذاری شده با استفاده از ابزار رمزنگاشتی
enciphered syn. encrypted	رمزگذاری‌شده، رمزیده	داده‌های رمزشده
enciphered code	کد رمزگذاری، کد رمزیده	کدی که تبدیل به رمز شده باشد و معنای آن برای گیرندهٔ غیرمجاز قابل درک نباشد.
enciphering syn. encryption	رمزگذاری	فرایند تبدیل متن اصلی به متن رمزشده با استفاده از خوارزمی(الگوریتم) رمزنگاشتی
encrypt syn. encipher	رمزگذاری کردن	تبدیل متن اصلی به متن رمزشده با استفاده از ابزار رمزنگاشتی
encrypted syn. enciphered	رمزگذاری‌شده، رمزیده	داده های رمزشده
encrypted data	داده‌های رمزگذاری‌شده، داده‌های رمزیده	داده‌های تغییرداده‌شده با استفاده از یک سامانهٔ رمزنگاشتی که برای اشخاص یا طرف‌های غیرمجاز مفهوم نباشد

واژه بیگانه	معادل فارسی	تعریف
encryption syn. enciphering	رمزگذاری	فرایند تبدیل متن اصلی به متن رمزشده با استفاده از خوارزمی(الگوریتم) رمزنگاشتی
encryption algorithm syn. cipher	خوارزمی رمزگذاری ، الگوریتم رمزگذاری مت.رمز	خوارزمی/ الگوریتمی برای تبدیل متن اصلی به متن رمزگذاری‌شده به‌نحوی که برای گیرندهٔ غیرمجاز غیرقابل‌درک باشد
end-to-end encryption	رمزگذاری سرتاسر	رمزگذاری اطلاعات در مبدأ و رمزگشایی آن در مقصد، بدون امکان رمزگشایی در نقاط میانی
end-to-end security	امنیت سرتاسر	محافظت از اطلاعات در یک سامانهٔ اطلاعاتی از نقطهٔ مبدأ تا نقطهٔ مقصد
entrapment	تله‌گذاری	تعبیهٔ عمدی رخنه‌های مشخص در یک سامانهٔ اطلاعات با هدف آشکارسازی 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	حملهٔ دورزنی	حمله‌ای که در آن مهاجم بدون آنکه افزاره امنیتی متصل به شبکه یا سامانهٔ هدف متوجه شود از آن عبور می‌نماید
exhaustive key search syn. brute force attack	کلیدجویی فراگیر مت. حملهٔ غیرهوشمندانه	حمله‌ای مبتنی بر آزمایش و به‌کارگیری تک‌تک کلیدها به‌منظور 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، به‌جز 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 syn. fail-stop signature	امضای رقمی جعل-اثبات مت. امضای جعل-اثبات

نوعی امضای رقمی که در آن امضاکننده از جعل‌ناپذیری امضای خود به‌صورت بی‌قید وشرط اطمینان می‌یابد و درصورت مشاهدهٔ امضایی که خود تولید نکرده است، می‌تواند جعلی بودن آن را اثبات کند؛ درحالی‌که وارسی‌کننده 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 جعل‌ناپذیری امضای خود به‌صورت بی‌قید وشرط اطمینان می‌یابد و درصورت مشاهدهٔ امضایی که خود تولید نکرده است می‌تواند جعلی بودن آن را اثبات کند؛ درحالی‌که وارسی‌کننده با خطر تأیید امضای جعلی مواجه است و اطمینان او از اعتبار امضا تنها به شیوهٔ محاسباتی برآورده می‌شود

واژه بیگانه	معادل فارسی	تعریف
fast correlation attack	حملهٔ همبستگی سریع	

نوعی حملهٔ همبستگی که به علت استفاده از فنون تصحیح خطای کارا (efficient error-correcting techniques) و اجتناب از جستجوی کامل حالت-های اولیه، به میزان قابل‌توجهی از حملهٔ همبستگی سریع‌تر است

fault attack	حملهٔ عیب‌افزایشی	

هر نوع حمله با استفاده از ترکیبی از شرایط محیطی مختلف که سبب ایجاد خطاهای محاسباتی در تراشه و درنتیجه نشت اطلاعات حفاظت‌شده می‌شود

feedback shift register (FSR)	ثبّات انتقال بازخوردی(ثاب)	

ساختاری متشکل از دو بخش شامل یک ثبّات انتقال و یک تابع بازخورد که به عنوان عنصر اصلی مولد کلید اجرایی در رمز جریانی به کار می‌رود

filter generator	مولد پالایه‌ای	

نوعی مولد کلید جریانی برای خوارزمی/ الگوریتم های رمز جریانی، متشکل از یک ثاب خطی(ثبّات انتقال بازخوردی خطی) که خروجی آن از اعمال یک تابع غیرخطی بر روی برخی از حالت‌های ثبّات 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 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 پیش تصویر	

یکی از خصوصیات مطلوب در توابع چکیده‌ساز که باعث می‌شود به‌ازای هریک از مقادیرِ خروجی یک تابع چکیده‌ساز، یافتن دست‌کم یک ورودی که به آن مقدار خروجی تصویر شود، ازنظر محاسباتی عملی نباشد

واژه بیگانه	معادل فارسی	تعریف
fixed point attack	حملهٔ نقطه‌ثابتی	

حمله‌ای علیه توابع چکیده‌ساز که در آن برای یافتن برخورد، از نقطهٔ ثابت در زیرتابع (subfunction) فشرده‌ساز مورد استفاده در تابع چکیده‌ساز، استفاده می‌شود

flooding attack	حملهٔ سیلابی	

حمله‌ای با 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 افشای کلید یک نشست تنها بر امنیت همان نشست تأثیر گذارد و تهدیدی برای امنیت نشست‌های پیشین نباشد

freshness attack syn. replay attack	حملهٔ 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 abbr. FNVM attacker	مهاجم تام‌آگاه از حافظهٔ غیرفرّار	

مهاجمی که قادر به استخراج تمام اطلاعات سرّی ذخیره شده در حافظهٔ غیرفرّار است

fully memory leakage resilient protocol abrr. FMLR protocol	قرارداد تام‌نشت‌تاب حافظه اختصار: قرارداد تام‌نشتاب	

قراردادی(پروتکلی) که حتی در صورت نشت کامل اطلاعات از حافظهٔ غیرفرّار همچنان امن است

functional encryption	رمزگذاری تابعی	

نوعی رمزگذاری نامتقارن که در آن هر کاربر مجاز، با استفاده از یک کلید خصوصی، قادر به دستیابی به تابعی مشخص از متن اصلی می‌شود

واژه بیگانه	معادل فارسی	تعریف

G

gap ریسهٔ صفر

دنباله‌ای ازصفرهای متوالی در یک دنبالهٔ دودویی که بیت پیش و پس از آن یک باشد

gap Diffie-Hellman group گروه گسست دیفی ـ هلمن

گروهی که حل مسئلهٔ تصمیم دیفی ـ هلمن روی آن در زمان چندجمله‌ای امکان پذیر باشد، اما احتمال وجود یک خوارزمی/ الگوریتم احتمالاتی برای حل مسئلهٔ محاسباتی دیفی ـ هلمن بر روی آن در زمان چند جمله‌ای ناچیز باشد

gap Diffie-Hellman problem
abbr: GDH problem
مسئلهٔ گسست دیفی ـ هلمن

مسئلهٔ پیدا کردن عنصر $c = g^{ab}$ با فرض در اختیار داشتن سه تایی (g^b, g^a, g) و نیز با فرض توانایی حل مسئلهٔ تصمیم دیفی- هلمن

generalized inversion attack حملهٔ وارونی تعمیم‌یافته

نوعی حملهٔ وارونی که بر همهٔ مولدهای پالایه‌ای، اعم از خطی و غیرخطی، قابل‌اجرا است

group authenticator اصالت‌نشان گروهی

ابزاری که دسترسی به برخی داده‌ها یا منابع به‌اشتراک‌گذاشته‌شده را برای اعضای یک گروه مشخص فراهم می‌کند

group computational Diffie–Hellman assumption
abr. GCDH
فرض محاسباتی دیفی–هلمن گروهی

فرضی که براساس آن محاسبهٔ راز دیفی–هلمن گروهی توسط یک مهاجم با قدرت محاسباتی محدود، با در اختیار داشتن مقادیر $g^{\prod x_i}$ برای زیرمجموعه‌های مناسب از {1, …,n} دشوار باشد، که در آن g مولد یک گروه دوری G و $x_i \in [1, |G|]$ است

group key agreement
syn. group key distribution
توافق کلید گروهی
مت. توزیع کلید گروهی

صورت گسترش‌یافتهٔ توافق کلید که در آن کلید مشترک بین چند نهاد به اشتراک گذاشته می‌شود

واژه بیگانه	معادل فارسی	تعریف
group key distribution syn. group key agreement	توزیع کلید گروهی مت. توافق کلید گروهی	

صورت گسترش‌یافتهٔ توافق کلید که در آن کلید مشترک بین چند نهاد به اشتراک گذاشته می‌شود

group signature	امضای گروهی

نوعی امضای رقمی که در آن هریک از اعضای گروهِ تشکیل‌شده، از جانب آن گروه و به‌طور گمنام، قادر به تولید امضا باشند. مدیر گروه یک هستار معتمد است که بر خروج یا ورود افراد جدید نظارت می‌کند و در صورت لزوم قادر به شناسایی امضاکننده است

H

hardware security module abbr. HSM	پودمان امنیتی سخت‌افزاری اختصار: پاس

افزارهٔ محاسباتی فیزیکی مقاوم در برابر دستکاری و نفوذ، برای حفاظت و مدیریت کلیدهای رقمی و سایر رازها، و همچنین، پردازش‌های رمزنگاشتی

hash-based cryptography	رمزنگاری چکیده‌بنیاد

نوعی رمزنگاری مبتنی بر نخستینه‌های (primitives) رمزنگاشتی، که امنیت آن‌ها بر امنیت توابع چکیده‌ساز استوار است

hash-based message authentication code abbr. 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. الگوربتم 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

واژه بیگانه	معادل فارسی	تعریف
hashing algorithm syn. cryptographic hash function syn. hash function	الگوربتم 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 نتیجهٔ تلاش ناموفق شمار بسیاری از افراد حرفه‌ای برای شکستن یک سامانهٔ رمز
homophonic substitution cipher	رمز جانشینی هم‌نوا	نوعی رمز جانشینی که در آن هر حرف متن اصلی به حرفی از یک مجموعهٔ چندتایی از حروف الفبای رمز نگاشته می‌شود
hot storage	انبارهٔ گرم	افزاره‌ای الکترونیکی متصل به اینترنت، برای ذخیرهٔ ارزهای رقمی/ دیجیتال، که معمولاً راه‌اندازی و دسترس‌پذیری و مقیاس‌پذیری آن در مقایسه با انبارهٔ سرد آسان‌تر است، اما در برابر دسترسی غیرمجاز و حملات رخنه‌گری (hacking attacks) و سایر آسیب‌پذیری‌ها ضعیف‌تر است
hot wallet	انبارهٔ گرم	نوعی کیف رمزارز، همیشه متصل به اینترنت یا افزاره‌های دیگر، که برای ذخیره‌سازی موقت کلید و ارسال و دریافت رمزارزها به‌کار می‌رود
hybrid encryption	رمزگذاری ترکیبی	نوعی رمزگذاری که از ترکیب دو یا چند خوارزمی/ الگوریتم رمزگذاری حاصل می‌شود و غالباً ترکیبی از رمزگذاری متقارن و نامتقارن است

I

ID-based access control	واپایش دسترسی شناسه‌بنیاد	نوعی واپایش دسترسی مبتنی بر شناسهٔ کاربر

واژه بیگانه	معادل فارسی	تعریف
identity-based cryptosystem syn. ID-based cryptosystem	سامانه رمز شناسه‌بنیاد	نوعی سامانهٔ 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 شناسهٔ متناظر با او مانند نشانی رایانامه یا نام کاربر یا شمارهٔ تلفن قابل تولید است
identity-based encryption abbr. IBE	رمزگذاری شناسه‌بنیاد	نوعی طرح رمزگذاری کلید عمومی که در آن کلید عمومی براساس اطلاعاتی یکتا از هویت کاربر تولید می‌شود
identity-based key exchange protocol	قرارداد تبادل کلید شناسه‌بنیاد	یک قرارداد تبادل کلید ساده که برای شبکه‌هایی با اندازهٔ دلخواه قابل‌اجراست و در آن هر کاربر جدید تنها با یک بار مراجعه به یک مرکز احراز اصالت کلید می‌تواند کلیدهای احرازاصالت‌شده را با کاربران دیگر شبکه مبادله کند
identity-based public-key cryptography	رمزنگاری کلیدعمومی شناسه‌بنیاد	مجموعه‌ای از نخستینه‌های رمزنگاشتی کلید عمومی که در آن کلیدهای عمومی تنها از اطلاعات شناسهٔ کاربران تشکیل شده است و مزیت آن کاهش نیاز به گواهی‌های رقمی برای ایجاد ارتباط بین کلیدهای عمومی و شناسهٔ کاربر متناظر است
identity-based signature	امضای شناسه‌بنیاد	نوعی طرح امضا، متشکل از چهار خوارزمی/ الگوریتم برپایی، اشتقاق کلید و امضا و وارسی، که در آن در مرحلهٔ برپایی یک مرکز تولید کلید مورداعتماد یک جفت شاه‌کلید عمومی و خصوصی تولید می‌کند و سپس، کلید خصوصی هر کاربر را این مرکز با استفاده از خوارزمی/ الگوریتم اشتقاق کلید بر مبنای شناسهٔ کاربر و شاه‌کلید خصوصی تولید می‌کند
identity binding	ترابست شناسه	ایجاد ارتباط بین هویت یک فرد با شناسهٔ ادعایی توسط یک مرجع رسمی
identity proofing	اثبات شناسه	فرایند ارائه و تأیید اطلاعات کافی برای شناسایی منحصربه‌فرد هر فرد از سوی مراجع ثبت گواهی و صدور اعتبارنامه
identity registeration	ثبت شناسه	فرایند معرفی شناسهٔ یک شخص به سامانهٔ وارسی شناسهٔ شخصی با استفاده از یک شناسانهٔ منحصربه‌فرد متناظر

واژه بیگانه	معادل فارسی	تعریف
imitative communications deception	فریب ارتباطاتی بدلی	تزریق پیام یا نشانک‌های/ سیگنال‌های فریب‌آمیز به نشانک‌های/ سیگنال‌های ارتباطاتی مهاجم
impersonation attack	حملهٔ جعل هویت	حمله‌ای که در آن مهاجم هویت یکی از طرف‌های مجاز در یک سامانه یا پروتکل (قرارداد) ارتباطی (communications protocol) را به خود نسبت می‌دهد
implicit key authentication syn. key authentication	احراز اصالت ضمنی کلید، اصالت‌سنجی ضمنی کلید مت. احراز اصالت کلید، اصالت‌سنجی کلید	فرایند معمول در طرح‌های برقراری کلید برای تضمین عدم دستیابی هستاری دیگر، به جز هستار مورد نظر، به کلید
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 انکارناپذیری
information warfare abrr. IW	جنگ اطلاعاتی	عملیاتی با هدف تخریب یا دستیابی به منابع اطلاعاتی طرف مقابل(قربانی)
information-theoretically secure steganography	نهان‌نگاری نظریه‌اطلاعاتی‌امن	نوعی نهان نگاری با ویژگی امن کامل یا امن آماری
integer counter mode syn. counter mode	شیوهٔ شمارگر صحیح مت. شیوهٔ شمارگر	یکی از روش‌های معیار به‌کارگیری رمز قالبی (block cipher) که در آن ابتدا دنباله‌ای از اعداد به‌عنوان ورودی خوارزمی/ الگوریتم رمز وارد می‌شود، سپس قالب‌های متن اصلی به‌ترتیب با قالب‌های خروجی خوارزمی /الگوریتم رمز ترکیب می‌شوند تا متن رمزشدهٔ متناظر با هر قالب به دست آید؛ پس از رمزگذاری هر قالب به مقدار شمارگر، مقدار ثابتی، معمولاً یک واحد، افزوده می‌شود

واژه بیگانه	معادل فارسی	تعریف
integrity check value abrr. ICV	قدرآزمای یکپارچگی	نوعی جمع‌آزما (checksum) با قابلیت کشف تغییر در یک سامانهٔ اطلاعاتی
Internet Key Exchange abbr. IKE	تبادل کلید اینترنت اختصار: تکا	نوعی قرارداد تبادل کلید احرازاصالت‌شده، مبتنی بر RFC2409، که از ترکیب قراردادهای Oakley و ISAKMP برای برقراری یک مجرای امن در اینترنت ایجاد شده است
internet protocol security abbr. IP Security, IPsec	امنیت قرارداد اینترنت	نوعی قرارداد استاندارد برای تأمین احراز اصالت و رمزگذاری ارتباطات از طریق اینترنت
intractable problems	مسائل مهارناپذیر	مسائلی که در زمان چندجمله‌ای قابل‌حل نیستند، زیرا محاسبهٔ جواب آن‌ها به‌سرعت غیرعملی می‌شود
invasive attack	حملهٔ تهاجمی	حمله به سامانه‌های فیزیکی که در نتیجهٔ آن ویژگی‌های فیزیکی تراشه به طور برگشت‌ناپذیر تغییر می‌کند
inversion attack	حملهٔ وارونی	نوعی حمله با متن اصلی معلوم به برخی مولدهای پالایه‌ای، برای بازیابی حالت اولیهٔ ثاب خطی(ثّبات انتقال بازخوردی خطی) از یک قطعه کلید جریانی، هرگاه چندجمله‌ای بازخوردی ثّبات و نقاط انشعاب و مولد پالایه‌ای معلوم باشند

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

واژه بیگانه	معادل فارسی	تعریف
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 مشارکت‌کننده 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 شاه‌کلید گره‌های موجود در شبکه را در اختیار دارد و همچنین قادر است کلید جلسه را برای همهٔ گره‌ها به‌صورت دوبه‌دو تولید کند

Key Encapsulation Mechanism
abrr. KEM — سازوکار لفاف‌بندی کلید
اختصار: سِلک

استفاده از رمزگذاری نامتقارن برای رمزگذاری یک کلید متقارن

key escrow — امانسپاری کلید

سپردن کلید رمزنگاشتی به یک یا چند نهاد ثالث معتبر برای بازیابی آن تحت شرایط خاص

key establishment — برقراری کلید

روند توزیع امن کلیدهای رمزنگاشتی بین پودمان‌ها

key exchange — تبادل کلید

به اشتراک گذاشتن یک کلید مخفی بین طرفین برای برقراری یک ارتباط امن

تعریف	معادل فارسی	واژه بیگانه
	گسترش کلید	key expansion
روالی برای تولید کلیدهای دور یا زیرکلیدها (sub- keys) از کلید رمز یا کلید اصلی (main key)		
	طولِ عمر کلید مت. رمزدوره	key lifetime syn. crypto period
بازه‌ای زمانی که در آن کلید رمزگزاری برای یک سامانهٔ رمز معتبر است		
	افزارهٔ مدیریت کلید	key management device
افزاره‌ای که توزیع امن کلیدهای رمزنگاشتی را به صورت الکترونیکی برای کاربران مجاز فراهم می‌کند		
	زیرساخت مدیریت کلید	key management infrastructure
همهٔ بخش‌های مربوط به پشتیبانی و تهیهٔ ملزومات لازم برای مدیریت کلید شامل سخت‌افزار و ثابت‌افزار و نرم‌افزارهای رایانه‌ای و دیگر تجهیزات و مستندات		
	مذاکرهٔ کلید	key negotiation
فرآیند برپایی کلید نشست سرّی برای تبادل امن داده بین طرفین ارتباط		
	زوج‌کلید	key pair
دو کلید که با یکدیگر رابطهٔ 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		
	بازیابی کلید	key recovery
تولید مجدد کلید رمزنگاشتی در صورت سرقت یا گم شدن یا تخریب آن		
	حملهٔ بازیابی کلید	key recovery attack
نوعی حمله به قصد یافتن کلید یک سامانهٔ رمز		

واژه بیگانه	معادل فارسی	تعریف
key schedule	فرانمای کلید	

الگوریتمی برای تولید زیرکلیدها در دورهای مختلف یک رمز قالبی، با استفاده از کلید منتخب کاربر

keystream/ key stream/ key-stream syn. running-key	جریان‌کلید متـ. کلید جریانی

دنباله‌ای که در رمزهای جریانی نماد به نماد با دنبالهٔ متن ساده ترکیب می‌شود تا دنبالهٔ 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	کلیدگذاری

جانشانی کلید در یک ابزار رمزنگاشتی

keystream/ key stream/ key-stream	جریان‌کلید

دنباله‌ای مورد استفاده در رمزهای جریانی که از ترکیب نماد به نماد اعضای آن با عناصر دنبالهٔ متن اصلی، دنبالهٔ متن رمز به دست می آید

kleptography	سرقت‌شناسی

بررسی چگونگی دستیابی طراح یک سامانهٔ رمز به اطلاعات کاربران بدون اطلاع آن‌ها

knapsack problem	مسئلهٔ کوله‌پشتی

مسئلهٔ یافتن زیرمجموعه‌ای از یک مجموعه اعداد صحیح مثبت، که حاصل‌جمع اعضای آن برابر با یک عدد مشخص باشد

known-plaintext attack	حمله با متن اصلی معلوم

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

واژه بیگانه	معادل فارسی	تعریف
known related key attack	حملهٔ کلیدمرتبط معلوم	

حملهٔ کلیدمرتبطی که بر پایهٔ آگاهی مهاجم از ارتباط بین کلیدها استوار است

known signature attack — حملهٔ امضامعلوم

حمله‌ای که تنها با در اختیار داشتن کلید عمومی امضاکننده و مجموعه‌ای از چند زوج پیام–امضا (message-signature pairs) صورت می‌گیرد

L

lattice-based cryptography — رمزنگاری مشبکه‌بنیاد

نوعی رمزنگاری که امنیت آن براساس سختی چند مسئلهٔ دشوار در حوزهٔ مشبکه‌ها استوار است

ledger — دفترکل

کتابی (دفتری) به‌صورت رقمی/ دیجیتالی یا کاغذی برای ثبت منظم رویدادها و امور مختلف، به‌ویژه فعالیت‌های تجاری و مبالغ دریافتی یا پرداختی

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

نوعی ثبّات 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

واژه بیگانه	معادل فارسی	تعریف
linear feedback shift register syn. LFSR	ثبّات انتقال بازخوردی خطی مت. ثاب خطی	نوعی ثبّات انتقال بازخوردی که تابع بازخورد آن خطی است
linear syndrome attack	حملهٔ نشانگان‌خطی	نسخه‌ای ضعیف از حملهٔ همبستگی سریع که بر روی مولدهای جریان کلید مبتنی بر ثاب خطی اعمال می‌شود
linguistic steganography	نهان‌نگاری زبانی	هنر پنهان‌سازی 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 رمزگشائی، در مسیریاب‌ها ضروری است
logical attack	حملهٔ منطقی	حمله‌ای با هدف بازیابی داده‌های سرّی از تجهیزات امن بدون آسیب‌رسانی جدی به آنها

M

malicious node	گره بدخواه	گرهی با هدف منع خدمت یا ایجاد اخلال در عملکرد شبکه که از طریق تغییر مشخصه‌های شبکه یا تغییر داده‌ها، پیش، یا درهنگام انتقال یا پس از آن عمل می‌کند
Malleability	چکش‌پذیری	خاصیت یک خوارزمی/ الگوریتم که به‌موجب آن با داشتن متن رمزشدهٔ c_1 ، تولید یک متن رمزشدهٔ دیگر مانند c_2، با ارتباط معلوم بین متن‌های اصلی متناظر آنها امکان‌پذیر باشد
mandatory access control	واپایش دسترسی اجباری	نوعی واپایش برای محدودسازی دسترسی به منابع، توسط مدیر شبکه براساس مجموعه‌ای از قوانین و مقررات الزامی

واژه بیگانه	معادل فارسی	تعریف
man-in-the-middle attack	حملهٔ فرددرمیان	حمله‌ای که در آن مهاجم در بین دو طرف یک مسیر امن قرار می‌گیرد و هر بار خود را به جای یکی از طرف‌ها معرفی می‌کند
manipulative communications deception	فریب ارتباطاتی ساختگی	تغییر یا شبیه‌سازی ارتباطات دوستانه به‌منظور فریب
master key	شاه‌کلید	کلیدی رمزنگاشتی که کاربرد اصلی آن محافظت یا تولید کلیدهای دیگر است
matrix embedding	نهفته‌سازی ماتریسی	روشی در کدگذاری که در نهان‌نگاری برای بهبود ظرفیت نهفته‌سازی با تغییرات کم در تصویردانه‌های تصاویر پوشانه، در مقایسه با دیگر طرح‌ها، به‌کار می‌رود
maximum disclosure proof	اثبات بیش‌تراوا مت. اثبات بیشینه‌افشا	نوعی روش اثبات در رمزنگاری که در آن اثبات‌کننده دارای اطلاعات وارسی‌پذیر است و برای متقاعد ساختن وارسی‌کننده به این واقعیت، اطلاعات را در اختیار او قرار می‌دهد، به‌طوری‌که وارسی‌کننده خود قادر به اجرای روند وارسی باشد
meet-in-the-middle attack	حملهٔ تلاقی‌درمیان	حمله‌ای که در آن مهاجم سعی می‌کند با داشتن تکه‌ای از متن رمزی‌شده 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 (سیلیسیمی)حافظه‌مبنا مت. تفت سیلیکونی حافظه‌مبنا	دسته‌ای از توابع فیزیکی تکثیرناپذیر سیلیکونی(سیلیسیمی) که خروجی آن‌ها از طریق اندازه‌گیری تغییرات مشخصه‌های تصادفی، که بین افزاره‌های سیلیکونی(سیلیسیمی) مشابه در عناصر حافظه‌های دوحالتی وجود دارد، به دست می‌آید

واژه بیگانه	معادل فارسی	تعریف
message authentication code abbr. MAC	کد احراز اصالت پیام، کد اصالت‌سنجی پیام اختصار: کاپ	نوعی جمع‌آزمای رمزنگاشتی مبتنی بر رمزنگاری متقارن برای کشف تغییرات رخ-داده بر روی داده‌ها، اعم از عمدی و تصادفی
message digest	چکیده‌پیام	نسخهٔ فشرده‌شدهٔ یک پیام اصلی که با استفاده از خوارزمی/ الگوریتم چکیده‌ساز تولید می‌شود
minimum disclosure proof	اثبات کم‌تراوا مت. اثبات کمینه‌افشا	نوعی روش اثبات در رمزنگاری که در آن اثبات‌کننده بدون هیچ شبهه‌ای می‌تواند وارسی‌کننده را به صحت اطلاعات خود متقاعد کند به طریقی که وارسی‌کننده نتواند از محتوای این اطلاع باخبر شود
mirror attack syn. reflection attack	حملهٔ بازتابی	نوعی حملهٔ تکرار که در آن مهاجم با قطع ارتباط، پیام ارسالی توسط یکی از دو طرف ارتباط را به خود او باز می‌گرداند
miss in the middle attack	حملهٔ بی‌تلاقی درمیان	روشی برای یافتن تفاضل‌های ناممکن در خوارزمی/ الگوریتم رمز که طرح اولیهٔ آن یافتن زوج‌متن‌هایی است که نتایج میانی حاصل از اعمال فرایند خوارزمی‌ها/ الگوریتم‌های رمزگذاری و رمزگشایی بر روی آن‌ها با هم تطبیق پیدا نمی‌کنند
mix network syn. mixnet	شبکهٔ مخلوط	سامانه‌ای برای گمنام‌سازی فرستندگان پیام با استفاده از عملیات رمزنگاشتی و جایگشتی در چند مرحله
Mobile Internet Key Exchange abbr.: MOBIKE	تبادل کلید اینترنت سیار اختصار: تکای سیار	نوعی تبادل کلید اینترنت (تکا) که استفاده از افزاره‌هایی با چند واسط شبکه با قابلیت جابه‌جایی از یک شبکه به شبکه دیگر را در زمان به‌کارگیری امنیت قرارداد اینترنت پشتیبانی می‌کند

واژه بیگانه	معادل فارسی	تعریف
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

monotone signature امضای یکنوا

نوعی امضای رقمی که تاحدی امکان مقاومت در برابر حملات باج‌خواهی (blackmailing attacks) را فراهم می کند. در این امضا، هر کاربر مجاز، ℓ زوج‌کلید $\{ski,pki\}$ تولید و برای امضای پیام‌های خود از آخرین کلید خصوصی، $sk\ell$، استفاده می‌کند؛ همچنین امضای تولیدشده با کلید خصوصی iام، ski، با استفاده از کلیدهای عمومی pkj، به‌ازای هر $j\leq i$ قابل‌وارسی است؛ ازاین‌رو، درصورت باج‌گیری، امضاکننده می‌تواند کلید ski را افشا کند و به کاربران اطلاع دهد که کلید عمومی pki فسخ شده و برای وارسی امضاها از کلید عمومی بعدی، $pki+1$، استفاده شود. به‌این‌ترتیب، مهاجم پس از اعلام فسخ کلید، درصورت دستیابی به کلید خصوصی ski، قادر به تولید امضای معتبر نخواهد بود

m-resilient m-تابا

نوعی تابع بولی که، حتی در صورت ثابت نگاه داشتن m متغیر ورودی آن، ویژگی توازن آن حفظ شود

m^{th} order correlation-immune Boolean function تابع بولی همبستگی‌ایمن مرتبهٔ 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 وارس‌مشخص

نوع تعمیم‌یافته‌ای از امضای وارس‌مشخص که در آن وارسی 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 وکلا با آستانهٔ تعیین‌شده برابر است

multiset attack حملهٔ بیش‌مجموعه‌ای

حمله‌ای عام به رمزهای متقارن، که برخلاف حملهٔ تفاضلی که در آن تنها رفتار یک زوج از متن‌های ورودی و خروجی توسط تحلیلگرمورد توجه قرار می گیرد، مجموعه‌ای بزرگتر و به دقت انتخاب شده مد نظر قرار می گیرد که بخش‌هایی از متن های ورودی آن تشکیل یک بیش‌مجموعه می‌دهند

تعریف	معادل فارسی	واژه بیگانه
	چندامضایی	multisignature

نوعی امضای آستانه‌ای که در آن گمنامی امضاکنندگان حفظ نمی‌شود

	سامانهٔ رمزکلید عمومی چندمتغیره	multivariate public-key cryptosystem

نوعی سامانهٔ رمز کلیدعمومی که امنیت آن مبتنی بر سخت بودن حل چندجمله‌ای‌های چندمتغیرهٔ غیرخطی بر روی یک میدان متناهی است

N

	تابع چشم‌پوشی‌پذیر	negligible function

تابعی مانند $r:\mathrm{N}\to\mathrm{N}$ که به‌ازای هر تابع چندجمله‌ای مانند $p:\mathrm{N}\to\mathrm{N}$، عدد صحیح مثبتی مانند k_0 وجود دارد که:

$$r(k)<1/p(k) \text{ for all } k\geq k_0$$

	ثاب غیرخطی	NLFSR
	مت. ثبّات انتقال بازخوردی غیرخطی	syn. nonlinear feedback shift register

نوعی ثبّات انتقال بازخوردی که تابع بازخورد آن غیرخطی است

	ته‌نقش‌گذاری ناکور	non-blind watermarking
	مت. ته‌نقش گذاری محرمانه	syn. private watermarking

نوعی ته‌نقش‌گذاری که در آن برای آشکارسازی ته‌نقش، به کلید محرمانهٔ فرستنده و نشانک پوششی نیاز است

	تک‌بار	nonce

عدد یا رشته‌ای عددی که برای رویارویی با حملهٔ تکرار، تنها یک بار در یک الگوریتم یا پروتکل(قرارداد) رمزنگاشتی به کار می‌رود

واژه بیگانه	معادل فارسی	تعریف
non-interactive zero-knowledge proof	اثبات ناتراوای غیرتعاملی، اثبات دانش‌صفر غیرتعاملی	

روشی برای کاهش شمار دورها در یک اثبات ناتراوا با ارسال تنها یک پیام از طرف اثبات‌کننده به وارسی‌کننده همراه با تغییر مدل به‌طوری‌که یک رشتهٔ تصادفی مشترک مرجع در دسترس تمامی شرکت‌کنندگان در قرارداد قرار می‌گیرد و اثبات‌کننده یک تک‌پیام به وارسی‌کننده می‌فرستد

non-invasive attack — حملهٔ غیرتهاجمی

حمله به سامانه‌های فیزیکی با بهره‌گیری از اطلاعات دردسترس، مانند زمان اجرا و مصرف توان، بدون نیاز به تخریب تراشه

non-negligible function — تابع چشم‌پوشی‌ناپذیر

تابعی مانند $r:\mathrm{N}\to\mathrm{N}$ که برای آن تابع مقدار چندجمله‌ای $q(\cdot)$ موجود است که به‌ازای مقادیر به اندازهٔ کافی بزرگ k داشته باشیم: $r(k) \geq 1/q(k)$

nonlinear feedback shift register abbr. NLFSR — ثبّات انتقال بازخوردی غیرخطی؛ مت.ثاب غیرخطی

نوعی ثبّات انتقال بازخوردی که تابع بازخورد آن غیرخطی است

nonmalleability — چکش‌ناپذیری

خاصیت یک خوارزمی/ الگوریتم که به‌موجب آن با داشتن متن رمزشدهٔ c_1، تولید یک متن رمزشدهٔ دیگر مانند c_2، با ارتباط معلوم بین متن‌های اصلی متناظر آنها امکان‌پذیر نباشد

not negligible function — تابع ناچشم‌پوشی‌پذیر

تابعی مانند $r:\mathrm{N}\to\mathrm{N}$ که برای آن تابع مقدار چندجمله‌ای $q(\cdot)$ موجود است که به‌ازای تعداد نامتناهی از مقادیر k، رابطهٔ $r(k) \geq 1/q(k)$ برقرار باشد

non-transferable signature — امضای انتقال‌ناپذیر

نوعی امضای رقمی که تنها از طریق فردی که امضاکننده او را مشخص کرده باشد، قابل وارسی است

واژه بیگانه	معادل فارسی	تعریف

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 می‌کند، بدون آنکه قادر به تشخیص پیام مزبور از بین مجموعهٔ پیام‌ها باشد یا یک پیام را با استفاده از یکی از کلیدهای خصوصی خود، بدون تشخیص آن کلید امضا می‌کند

oblivious transfer
abbr. OT — انتقال ناآگاهانه

قراردادی(پروتکلی) بین فرستنده و گیرنده که براساس آن فرستنده اقدام به ارسال برخی از اطلاعات برای گیرنده می‌کند، بدون آنکه بداند گیرنده چه اطلاعاتی دریافت کرده است

one-more forgery — جعل امضای یکی‌بیش

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 یک‌بارمصرف

رمزی که در آن از کلید رمز تنها یک بار استفاده می‌شود به‌طوری‌که هر حرف یا نماد کلید برای رمز کردن یک نماد متن اصلی به کار می‌رود

one-way function — تابع یک‌طرفه

یک تابع ریاضی که محاسبه آن ساده، اما محاسبه وارون آن بسیار دشوار باشد

original signer — امضاکنندهٔ اصلی

فرد یا هر هستاری که حق امضای خود را به دیگری به‌عنوان امضاکنندهٔ وکالتی واگذار می‌کند

out-of-band authentication
abbr.: OOBA — احراز اصالت فراباندی
مت.اصالت‌سنجی فراباندی
اختصار: افراب

فرایندی برای احراز اصالت، مبتنی بر دو نشانک مختلف که از دو شبکه یا مسیر متفاوت ارسال می‌شوند

واژه بیگانه	معادل فارسی	تعریف
output feedback mode abbr. OFB mode	شیوهٔ بازخورد خروجی	

یکی از روش‌های به‌کارگیری رمز قالبی که به‌کارگیری آن، عملکردی مشابه با رمزهای جریانی را فراهم می‌سازد

P

pairing — زوج‌نگاشت

نگاشتی مانند $(e: G_1 \times G_2 \to G_t)$ با ویژگی‌های دوخطی بودن، ناتباهیدگی (non-degeneracy)، و محاسبه‌پذیری

partial preimage resistance — مقاومت در برابر پیش‌تصویر جزئی

خصوصیتی در توابع چکیده‌ساز که باعث می‌شود حتی با معلوم بودن بخش بزرگی از ورودی، بازیابی بخش باقیماندهٔ 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 مجموعه‌ای از کاربران، بدون نیاز به اطلاعات سایر کاربران، تأمین می‌شود

passive adversary — مهاجم غیرفعال

مهاجمی که فقط با جست‌وجو در اطلاعات قابل دسترس برخی طرف‌های قرارداد(پروتکل) و بدون تغییر دادن آنها، سعی در فهم اطلاعات ورودی دیگر طرف‌های قرارداد(پروتکل) دارد

passive cheater — فریب‌دهندهٔ غیرفعال

فریب‌دهنده‌ای که قرارداد را اجرا می‌کند، ولی سعی می‌کند اطلاعاتی بیش از آنچه در قرارداد آمده است به دست آورد

passive eavesdropper — شنودگر غیرفعال

شنودگری که فقط می‌تواند متن رمزشده را بخواند یا گوش دهد

passive penetration test — آزمون نفوذ غیرفعال

آزمونی برای کاوش مرزهای محدودهٔ هدف و بررسی ضعف‌های امنیتی در محیط هدف بدون قصد بهره‌گیری از دسترسی و بدون تأثیر منفی بر عملکرد عادی آن

واژه بیگانه	معادل فارسی	تعریف
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 همهٔ مستندات دردسترس (از قبیل طراحی سامانه، کد منبع و کتابچه‌های راهنما) و تحت محدودیت‌های خاص، سعی در دور زدن ویژگی‌های امنیتی یک سامانهٔ اطلاعاتی دارند

perfect forward secrecy abbr. PFS	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 abbr. perfect ZK proof	اثبات ناتراوای کامل، اثبات دانش‌صفر کامل	

روشی که در آن مقدار اطلاعاتی که از اثبات‌کننده به وارسی‌کننده نشت 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 کاملاًامن	

نوعی خوارزمی/ الگوریتم نهان‌نگاری که احتمال موفقیت هر مهاجم با قدرت محاسباتی نامحدود برای یافتن تمایز بین پوشانه و نهانه آن صفر است

physical attack	حملهٔ فیزیکی	

حمله‌ای مبتنی بر شیوه‌ها و ابزارهای فیزیکی به افزاره‌های رمزنگاشتی

physical unclonable function abbr. PUF	تابع فیزیکی تکثیرناپذیر اختصار: تفت	

تابعی مبتنی بر پیچیدگی بسیار زیاد ساختار یک سامانهٔ فیزیکی، برای نگاشت مجموعه‌ای از چالش‌ها به مجموعه‌ای از پاسخ‌ها

plaintext syn. clear text/ cleartext	متن آشکار مت. متن اصلی	

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

تعریف	معادل فارسی	واژه بیگانه
	مخاطرهٔ کلید متن‌اصلی ـ متن‌رمز	plaintext-ciphertext compromise

لو رفتن اطلاعات کلید با در اختیار داشتن یک زوجِ متن‌اصلی و متن‌رمز متناظر با آن

	مخاطرهٔ کلید متن‌اصلی ـ متن‌اصلی	plaintext-plaintext compromise

لو رفتن اطلاعات کلید که از تحلیل داده‌های حاصل از رمزگذاری دو متن اصلی P_1 و P_2 با یک کلید حاصل می‌شود

	رمز چند الفبایی مت. رمزگذاری چند الفبایی مت. رمز جانشینی چند الفبایی	polyalphabetic cipher syn. polyalphabetic encryption syn. polyalphabetic substitution cipher

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

	رمز جانشینی چندنویسه‌ای	polygram substitution cipher

نوعی رمز جانشینی که در آن قالب‌هایی از حروف متن اصلی جانشین قالب‌های متناظر در حروف متن رمز می‌شوند

	رمز جانشینی چندنگاره‌ای	polygraphic substitution cipher

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

	الگوریتم زمان‌چندجمله‌ای/ خوارزمی زمان‌چندجمله‌ای	polynomial time algorithm

خوارزمی/ الگوریتمی که زمان اجرای آن تابعی چندجمله‌ای از طول ورودی آن است

	پویشگر درگاه مت. پویشگر آسیب‌پذیری	port scanner syn. vulnerability scanner

برنامه‌ای رایانه‌ای که برای ارزیابی ضعف‌های امنیتی سامانه‌های رایانه‌ای و شبکه‌ها و برنامه‌های کاربردی یا نرم‌افزاری طراحی شده است

واژه بیگانه	معادل فارسی	تعریف
power analysis attack syn.simple power analysis attack syn.power consumption attack	حملهٔ 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 هریک از مقادیرِ خروجی یک تابع چکیده‌ساز، یافتن دست‌کم یک ورودی که به آن مقدار خروجی تصویر شود، ازنظر محاسباتی عملی نباشد

presentation attack	حملهٔ وانمودسازی

ارائهٔ یک دست‌ساخته یا مشخصه‌های انسانی به یک زیرسامانهٔ دریافت مشخصه‌های زیستی، به نحوی که قصد جلوگیری از شناسایی سامانه را داشته باشد

primitive element	عنصر اولیه

عضوی از مرتبهٔ 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^i نمایش داد

primitive polynomial	چندجمله‌ای اولیه

یک چندجمله‌ای تکین از درجهٔ m، مانند f برروی میدان F_q که $f(0) \neq 0$ و مرتبهٔ آن برابر با $q^m - 1$ باشد

primitive root	ریشهٔ اولیه

مولد گروه ضربی، به پیمانهٔ یک عدد صحیح n

private key cryptography syn. secret key cryptography	رمزنگاری با کلید مخفی

روشی برای رمزگذاری پیام که در آن برای رمزگذاری و رمزگشایی تنها از یک کلید استفاده می‌شود

واژه بیگانه	معادل فارسی	تعریف
private watermarking syn. non-blind watermarking	ته‌نقش گذاری محرمانه مت. ته نقش گذاری ناکور	

نوعی ته‌نقش‌گذاری که در آن برای آشکارسازی ته‌نقش، به کلید محرمانهٔ فرستنده و پوشانه نیاز است

proactive secret sharing — تسهیم راز پیش‌نگر

نوعی طرح تسهیم راز که در آن با به‌روزرسانی دوره‌ای سهم‌ها، خطر افشای راز در صورت لو رفتن سهم سهامداران کاهش می یابد

proactive security — امنیت پیش‌نگر

امنیتی که در آن بدون تغییر کلید عمومی، وتنها با تغییر دادن کلیدهای خصوصی اعضای گروه، از سوءاستفاده جلوگیری می‌شود

proactive threshold cryptography — رمزنگاری آستانه‌ای پیش‌نگر

نوعی طرح رمزنگاری که با استفاده از توابع رمزنگاری مختلف، کارسازان را قادر می‌سازد سهم جدید خود را از کلید مخفی با مشارکت یکدیگر و بدون افشای کلید مخفی محاسبه کنند

proactive threshold signature — امضای آستانه‌ای پیش‌نگر

نوعی طرح امضا که با استفاده از آن هریک از اعضای گروه مجاز است گروه را ترک کند یا به آن بپیوندد یا کلیدهای امضای خصوصی خود را به‌روز کند، بدون آنکه بر کلید عمومی گروه تأثیر بگذارد

probabilistic algorithm — خوارزمی احتمالاتی
مت. الگوریتم احتمالاتی

خوارزمی/ الگوریتمی با قابلیت پرتاب سکه یا، به عبارت دیگر، خوارزمی/ الگوریتمی با دسترسی به یک منبع تصادفی برای تولید بیت‌های تصادفی نا اریب که به‌طور مستقل و با احتمال 1/2 مقادیر 0 یا 1 تولید می کند

probabilistic encryption — رمزگذاری احتمالاتی

نوعی رمزگذاری که در آن هر بار عمل رمزگذاری یک پیام با استفاده از یک کلید ثابت، به تولید متن‌های رمز متفاوت می‌انجامد

واژه بیگانه	معادل فارسی	تعریف
probabilistic polynomial time adversary	مهاجم زمان‌چندجمله‌ای احتمالاتی	مهاجمی با توانایی اجرای خوارزمی‌ها/ الگوریتم‌های زمان‌چندجمله‌ای احتمالاتی
probabilistic polynomial-time algorithm	خوارزمی زمان‌چندجمله‌ای احتمالاتی مت. الگوریتم زمان‌چندجمله‌ای احتمالاتی	یک خوارزمی/ الگوریتم احتمالاتی با امکان اجرای حداکثر تعداد چندجمله‌ای عملیات
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
probabilistic signature scheme abr.: pps	طرح امضای احتمالاتی	نوعی طرح امضای مبتنی بر RSA که احتمال جعل امضای آن با احتمال موفقیت حل مسئلهٔ RSA تقریباً برابر است
processing complexity	پیچیدگی پردازشی	زمان لازم برای انجام یک حمله
product cipher syn. superencryption	رمز ترکیبی مت. اَبَررمزگذاری	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 در آن، هم وکیل و هم موکل نقش دارند و درنتیجه موکل نمی‌تواند به جای وکیل به‌صورت وکالتی امضا کند
provable security	امنیت اثبات‌پذیر	امنیت یک سامانهٔ رمزنگاری که بتوان الزامات امنیتی آن را در یک مدل تهاجمی به‌شکل صوری بیان کرد

واژه بیگانه	معادل فارسی	تعریف
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 resignature	بازامضای وکالتی	نوعی امضا که در آن وکیلی نسبتاً معتمد، امضای یک نهاد برروی یک پیام مشخص را به امضای نهادی دیگر برروی همان پیام تبدیل می‌کند؛ در حالی که این وکیل قادر به تولید امضا برروی پیام‌های دلخواه از سوی هیچ یک از این دو نهاد نیست
proxy ring signature	امضای حلقوی وکالتی	نوعی امضای وکالتی که در آن موکل به گروهی از وکلا برای تولید امضا وکالت می‌دهد، به طوری که هویت امضاکننده (وکیل) از دید مهاجم و حتی امضاکنندهٔ اصلی مخفی بماند
proxy signature	امضای وکالتی	نوعی امضای رقمی که در آن امضاکنندهٔ اصلی می‌تواند حق امضای خود را به صورت کارا و شفاف به وکیل واگذار کند
proxy signer	امضاکنندهٔ وکالتی	کسی که امضاکنندهٔ اصلی حق امضای خود را به او واگذار می‌کند
pseudorandom function	تابع شبه‌تصادفی	یک تابع تعینی(قطعی) مبتنی بر یک کلید و ورودی که از یک تابع واقعاً تصادفی برحسب ورودی تمایزناپذیر است
pseudorandom number generator abbr. PRNG	مولد اعداد شبه‌تصادفی	مولدی که پس از مقداردهی اولیه با هر مقدار تصادفی (به نام بذر) دنباله‌ای شبیه به یک دنبالهٔ تصادفی را تولید می‌کند، به‌طوری که یک ناظر بدون اطلاع از مقدار بذر نتواند دنبالهٔ مزبور را از دنبالهٔ تولیدشده توسط یک مولد واقعاً تصادفی تمیز دهد

واژه بیگانه	معادل فارسی	تعریف
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 وکالتی	

نوعی امضای رقمی با قابلیت واگذاری حق امضا از سوی امضاکنندهٔ اصلی به وکیل، به صورت کارا و شفاف

public-key infrastructure	زیرساخت کلید عمومی	

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

public-key stegosystem	سامانهٔ نهان‌نگاری کلید عمومی	

سامانه‌ای شامل سه خوارزمی/ الگوریتم احتمالاتی تولید کلید و کدگذاری(درج) وکدگشایی(آشکارسازی) که در آن خوارزمی/ الگوریتم تولید کلید پارامتر امنیتی را به‌عنوان ورودی دریافت و یک زوج کلید خصوصی و عمومی نهان‌نگاری را تولید می‌کند و خوارزمی/ الگوریتم کدگذاری با به‌کارگیری کلید عمومی، نهانه را تولید، و الگوریتم/خوارزمی کدگشایی با استفاده از کلید خصوصی، نهانه را کدگشایی می‌کند

public-key watermarking syn. asymmetric watermarking	ته‌نقش‌گذاری 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

واژه بیگانه	معادل فارسی	تعریف
quantum deniable authentication	احراز اصالت انکارپذیر کوانتومی مت. اصالت‌سنجی انکارپذیر کوانتومی	نوعی احراز اصالت انکارپذیر مبتنی بر تبدیل یکانی و تابع یک‌طرفهٔ 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 به‌صورت تصادفی به هر ورودی مقدار خروجی صحیحی را نسبت می‌دهد
receiver deniable encryption	رمزگذاری گیرنده‌انکارپذیر	نوعی رمزگذاری که در آن گیرنده بتواند دریافت پیام رمزشده را انکار کند
recipient anonymity	گمنامی گیرنده	عدم امکان شناسایی گیرندهٔ پیام ازطریق شنود، در یک سامانهٔ ارسال و دریافت پیام
re-encryption mixnet	شبکهٔ مخلوط بازرمزگذاری	نوعی شبکهٔ مخلوط که در آن ورودی‌های هر مرحله با استفاده از یک کلید عمومی مشترک رمزگذاری می‌شوند
reflection attack syn. mirror attack	حملهٔ بازتابی	نوعی حملهٔ تکرار که در آن مهاجم با قطع ارتباط، پیام ارسالی یکی از دو طرف ارتباط را به خود او باز می‌گرداند
rekeying	کلیدگذاری مجدد	روند تغییر کلید رمزگذاری در بخش‌های باقی‌ماندهٔ یک متن در حال رمزی شدن برای محدود کردن حجم داده‌های رمزگذاری‌شده با کلید پیشین

تعریف	معادل فارسی	واژه بیگانه
	حملهٔ کلید مرتبط	related key attack

حمله‌ای که در آن مهاجم با اطلاع از رابطهٔ بین چند کلید و دسترسی به توابع رمزگذاری متناظر در پی یافتن کلید است

	تحلیل رمز کلیدمرتبط	related-key cryptanalysis

نوعی تحلیل رمز مشابه با تحلیل تفاضلی رمز که در آن تفاضل بین کلیدها بررسی می‌شود

	حملهٔ بازِارسالی	relay attack

نوعی حملهٔ فرددرمیان 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

	حملهٔ تکرار	replay attack syn. freshness attack

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

	اثبات ناتراوایِ بازنشان‌پذیر، مت. اثبات دانش‌صفرِ بازنشان‌پذیر	resettable zero-knowledge proof

نوعی روش اثبات دانش‌صفر که حتی در صورت تعامل چندبارهٔ 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

	مرتبهٔ تابایی	resiliency order

بیشینه مقدار m که به ازای آن تابع f، m-تابا باشد

	امضای حلقوی	ring signature

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

	ریسه	run

بیت‌های یکسان متوالی در یک دنبالهٔ دودویی که با بیت‌های پیش و پس از خود متفاوت باشند

واژه بیگانه	معادل فارسی	تعریف
running-key syn. keystream/ key stream/ key-stream	کلید جریانی مت. جریان‌کلید	

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. برخوردتابی ضعیف

یکی از خصوصیات توابع چکیده‌ساز، که در صورت وجود آن، با در اختیار داشتن m_1، یافتن m_2 به‌طوری‌که $hash(m_2) = hash(m_1)$ دشوار باشد

secret handshake — دست‌داد سرّی

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

کلیدی که از آن در رمزنگاری متقارن استفاده می‌شود

secret key cryptography
syn. private key cryptography syn. 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 به‌طوری‌که زیرمجموعهٔ مشخصی از آنها قادر به بازیابی آن اطلاعات باشند درحالی‌که سایر اعضا قادر به درک هیچ‌گونه اطلاعات مرتبط با آن نباشند

واژه بیگانه	معادل فارسی	تعریف
secure socket layer abbr. SSL	لایهٔ اتصال امن اختصار: 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 reduction	تحویل امنیتی	بخشی از یک اثبات امنیتی (security proof) که بر چگونگی تبدیل شکستن یک طرح پیشنهادی به حل یک مسئلهٔ سخت تمرکز دارد
security specifications	مشخصات امنیتی	توصیف دقیق حفاظ‌های موردنیاز برای حفاظت از یک سامانهٔ اطلاعاتی
security strength	استحکام امنیتی	تعداد عملیات موردنیاز برای شکستن یک الگوریتم/خوارزمی یا سامانهٔ رمزنگاشتی
security tag	برچسب امنیتی	واحد اطلاعاتی که اطلاعات مرتبط امنیتی معینی را نمایش می‌دهد
security target	هدف امنیتی	مشخصات معیارهای مشترکی که نشان‌دهندهٔ مجموعه‌ای از نیازمندی‌های امنیتی است و بر مبنای آن ارزیابی امنیتی انجام می شود
seed key	بذرکلید	کلید اولیه‌ای که برای شروع فرایند تولید یا به‌روزرسانی کلید به‌کار گرفته می‌شود
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

واژه بیگانه	معادل فارسی	تعریف
semantic security	امنیت معنایی	عدم نشت هرگونه اطلاعات از متن رمزشده در مورد متن اصلی، فارغ از توان مهاجم و مستقل از معنای نهفته در رمزگذاری
semi-invasive attack	حملهٔ نیم‌تهاجمی	نوعی حمله به سامانه‌های فیزیکی که از نظر عملکرد در رده‌ای بین حمله‌های تهاجمی و غیرتهاجمی قرار می‌گیرد
sender anonymity	گمنامی فرستنده	در یک سامانهٔ پیام، عدم امکان شناسایی فرستندهٔ پیام ازطریق شنود
sender deniable encryption syn. deniable encryption	رمزگذاری فرستنده‌انکارپذیر مت. رمزگذاری انکارپذیر	نوعی رمزگذاری که در آن فرستنده بتواند در صورت لزوم رمزگذاری پیام ارسال شده را انکار کند
session key	کلید نشست	کلیدی که از آن برای رمزگذاری متقارن در یک نشست استفاده و سپس آن را نابود می‌کنند
short digital signature	امضای رقمی کوتاه/ امضای دیجیتالی کوتاه	نوعی امضای رقمی برای استفاده در محیط‌هایی با پهنای باند محدود که برای تأمین سطح امنیت k-بیتی، طول امضای تولیدشده کمینه مقدار ممکن، مثلا 2k بیت، باشد؛ این مقدار در امضاهای متداول استاندارد برابر با 4k است
signatory	صاحب‌امضا	شخص یا کشور یا نهادی که با داشتن زوج‌کلید عمومی و خصوصی مجاز به امضای رقمی یک معاهده یا سند رسمی است؛ این امضا با کلید خصوصی تولید و با کلید عمومی وارسی می‌شود و تعهداتی را برای امضاکننده ایجاد می‌کند
signature validation	اعتبارسنجی امضا	درستی‌سنجی یک امضای رقمی، به‌صورت ریاضی، و کسب اطمینان لازم از اعتبار کلید عمومی، مالکیت کلید خصوصی و غیره

واژه بیگانه	معادل فارسی	تعریف
signature verification	درستی‌سنجی امضا مت. وارسی امضا	

استفاده از یک خوارزمی/ الگوریتم امضای رقمی و یک کلید عمومی برای تعیین درستی یک امضا

signcryption	رمزامضا	

انجام هم‌زمان امضای رقمی و رمزگذاری مثل رمزنگاری با کلید عمومی

signee syn. signatory	امضاصاحب	.

شخص یا کشور یا نهادی که با داشتن زوج‌کلید عمومی و خصوصی مجاز به امضای رقمی یک معاهده یا سند رسمی است؛ این امضا با کلید خصوصی تولید و با کلید عمومی وارسی می‌شود و تعهداتی را برای طرفین ایجاد می‌کند

signer	امضاکننده	

فرد یا هر هستاری که متن یا محتوای رقمی را امضا می‌کند

silicon physical unclonable function abbr. silicon PUF	تابع فیزیکی تکثیرناپذیر سیلیکونی اختصار: تفت سیلیکونی	

دسته‌ای اصلی از توابع فیزیکی تکثیرناپذیر الکترونیکی که در تراشه‌های سیلیکونی (سیلیسیمی) 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, syn. monoalphabetic substitution cipher	رمز جانشینی ساده مت. رمز تک الفبایی مت. رمز جانشینی تک الفبایی	

نوعی رمز جانشینی که در آن هر حرف متن اصلی جانشین یک حرف متناظر از الفبای رمز می‌شود

واژه بیگانه	معادل فارسی	تعریف
slide attack	حملهٔ لغزشی	

حمله‌ای عام (generic attack) به رمزهای تکراری که در آن از رابطهٔ بین یک کلید با خودش بهره‌برداری می‌شود

software attack	حملهٔ نرم‌افزاری	

هر نوع حمله از طریق رخنه‌های موجود در نرم‌افزار با استفاده از یک کانال ارتباطی عادی

space complexity	پیچیدگی حافظه‌ای	

پیچیدگی محاسباتی یک خوارزمی/ الگوریتم به لحاظ حافظهٔ مورد نیاز برای اجرای آن

square attack	حملهٔ مربعی	

نوعی حملهٔ بیش‌مجموعه‌ای که اولین بار حین تحلیل رمز مربع شناسایی شد و در آن تحلیل‌گر به‌جای مطالعهٔ رفتار یک زوج از متن‌های اصلی، مجموعهٔ بسیار بزرگ‌تری از متن‌های رمز را بررسی می‌کند که در آن بخش‌هایی از متن ورودی، تشکیل یک بیش‌مجموعه 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 درصورتی ضروری است که یک یا چند عضو به گروه بپیوندد یا آن را ترک کند، یا زوج‌کلیدهای اختصاصی یک یا چند عضو به‌روزرسانی شوند

static keys	کلیدهای ایستا	

کلیدهایی که طول عمر نسبتاً زیادی دارند و در تعدادی از اجراهای یک خوارزمی/ الگوریتم مشترک هستند

statistical zero-knowledge proof syn.almost-perfect zero-knowledge	اثبات ناتراوای آماری، اثبات دانش‌صفر آماری مت. اثبات ناتراوای تقریباً کامل، اثبات دانش‌صفر تقریباً کامل	

اثباتی که در آن، برخلاف حالت‌های کلی اثبات‌ناتراوا، توزیع مکالمات واقعی با توزیع مکالمات شبیه‌سازی‌شده از نظر آماری تمایزناپذیر است؛ یعنی فاصلهٔ آماری میان توزیع‌ها ناچیز است

واژه بیگانه	معادل فارسی	تعریف
statistically secure steganography	نهان‌نگاری آماری‌امن	نوعی خوارزمی/ الگوریتم 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	سامانهٔ نهان‌نگاری	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
stegotext	نهانه	پیامی که از درج داده‌های پیام محرمانه در داخل داده‌های پوشانه ایجاد می‌شود
still imagery steganography	نهان‌نگاری تصویرساکن	پنهان کردن پیام محرمانه در داخل تصاویر رقمی
storage complexity	پیچیدگی انبارشی	ظرفیت انبارهٔ مورد نیاز برای انجام یک حمله
stream cipher	رمز جریانی	نوعی رمز متقارن که در آن با تولید رشته‌ای از بیت‌ها به نام جریان‌کلید و ترکیب آن با متن اصلی رمزگذاری انجام می‌شود
strict avalanche criterion	معیار بهمنی اکید	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

واژه بیگانه	معادل فارسی	تعریف
strong designated verifier signatures	امضای وارس‌مشخص قوی	

نوعی امضای وارس‌مشخص با دو ویژگی جعل‌ناپذیری و وارسی‌ناپذیری عمومی که در آن تولید امضا تنها توسط امضاکنندهٔ اصلی و وارسی امضا تنها توسط وارس تعیین‌شده امکان‌پذیر باشد

strong physical unclonable function abbr. strong PUF	تابع فیزیکی تکثیرناپذیر قوی اختصار: تفت قوی	

نوعی تابع فیزیکی تکثیرناپذیر غیرقابل‌پیش‌بینی، با شمار فراوان چالش و دسترسی واپایش‌نشدهٔ مهاجم به آن

subset sum problem	مسئلهٔ جمع زیرمجموعه‌ها	

مسئلهٔ یافتن زیرمجموعه‌ای از یک مجموعه اعداد صحیح مثبت، که حاصل‌جمع اعضای آن برابر با یک عدد مشخص باشد

substitution cipher	رمز جانشینی	

روشی ابتدایی برای رمزگذاری یک پیام که از طریق آن می‌توان یک حرفِ متن اصلی را جانشین یک و فقط یک حرف از الفبای رمز کرد

substitution-permutation network abbr. SPN	شبکهٔ جانشینی–جایگشتی	

رمز ترکیبی متشکل از تعدادی مرحله که هریک شامل توابع جانشینی و جایگشتی هستند

superencryption syn. product cipher	اَبَررمزگذاری مت. رمز ترکیبی	

رمزی که از ترکیب دو یا چند تابع رمزگذاری مختلف ساخته می‌شود

superincreasing knapsack syn. superincreasing knapsack problem	کوله‌پشتی اَبَرافزایشی مت. مسئلهٔ کوله‌پشتی اَبَرافزایشی	

نوعی مسئلهٔ کوله‌پشتی که در آن اعضای مجموعهٔ اعداد صحیح، یک دنبالهٔ اَبَرافزایشی باشند

superincreasing knapsack problem syn. superincreasing knapsack	مسئلهٔ کوله‌پشتی اَبَرافزایشی مت. کوله‌پشتی اَبَرافزایشی	

نوعی مسئلهٔ کوله‌پشتی که در آن اعضای مجموعهٔ اعداد صحیح، یک دنبالهٔ اَبَرافزایشی باشند

واژه بیگانه	معادل فارسی	تعریف
superincreasing sequence	دنبالهٔ اَبَرافزایشی	

بُرداری که مقدار هر مؤلفه‌اش از مجموع مقادیر مؤلفه‌های پیشین آن بزرگ‌تر باشد

super poly	اَبَر چندجمله‌ای	

یک چندجمله‌ای مانند p_I در رابطهٔ

$P(x_1, \dots, x_n) \equiv t_I . p_I + q(x_1, \dots, x_n)$

که نمایشی از چندجمله‌ای $p(x_1, \dots, x_n)$ براساس متغیرهای منتخب I روی GF(2) است و هر جمله در $q(x_I \dots x_n)$ حداقل شامل یکی از متغیرهای مجموعهٔ I نیست

Sybil attack	حملهٔ سی‌بل، حملهٔ چندشناسه‌ای	

نوعی حمله در شبکه‌های همتابه‌همتا (peer-to-peer networks) که در آن یک گره از شبکهٔ 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 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 زیرمجموعهٔ t، عضوی از یک مجموعهٔ n عضوی از هستارها یا کارسازها، امکان رمزگشایی یک متن رمزشده را فراهم می‌سازد، درحالی‌که مانع از رمزگشایی پیام مزبور توسط هر زیرمجموعه با کمتر از t عضو می‌شود

واژه بیگانه	معادل فارسی	تعریف

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 اندازهٔ ازقبل‌تعیین‌شده(آستانه)، قادر به تولید یک امضای وکالتی معتبر از سوی وی باشد در حالی‌که زیرمجموعه‌های با تعداد کمتر از آستانهٔ تعیین‌شده 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 ازطرف کل گروه باشند

time complexity — پیچیدگی زمانی

پیچیدگی محاسباتی یک خوارزمی/ الگوریتم به لحاظ زمان مورد نیاز برای اجرای آن

time element scrambler — درهم ریز عنصر زمان
abbr.: time scrambler — درهم‌ریز زمانی

ابزاری برای تقسیم نشانک/ سیگنال قیاسی به دوره‌های زمانی مساوی به‌نام قاب زمانی و بازتقسیم هر قاب به زیردوره‌های زمانی کوچک مساوی به‌نام قطعه، سپس درهم ریختن نشانک/ سیگنال ورودی با تغییر جایگاه قطعه‌ها در داخل هر قاب

time-memory trade-off attack — حملهٔ بده‌بستان زمان ـ حافظه

اگر پیچیدگی یافتن کلید برابر با K باشد، در حملهٔ بده‌بستان زمان‌ـ 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 ـ حافظه ـ 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

time stamp — مهر زمانی

مجموعه‌ای از نویسه‌ها یا اطلاعات رمزگذاری‌شده که زمان وقوع یک رویداد خاص را مشخص می‌کند

واژه بیگانه	معادل فارسی	تعریف
time-stamping	مهرزنی زمانی	

فرایندی برای وارسی 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	حملهٔ 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 مهارپذیر	

مسائلی که معمولاً به‌ازای ورودی‌هایی با اندازهٔ معقول و با استفاده از خوارزمی‌ها/ الگوریتم‌های زمان‌چندجمله‌ای در یک زمان مناسب قابل‌حل هستند

traffic flow confidentiality abbr.: TFC syn.: Traffic Flow Confidentiality (TFC) mechanisems	محرمانگی جریان ارتباط	

خدمتی برای حفاظت از اطلاعاتی که ممکن است از مشاهدهٔ جریان ارسال و دریافت بسته‌های داده (ترافیک) به‌دست آیند

transitive signature	امضای تراگذر، امضای ترایا	

نوعی امضا که با در اختیار داشتن امضای روی یال‌های (a , b) و (b , c) از یک گراف، امکان تولید امضا روی یال (a , c) را بدون در اختیار داشتن کلید خصوصی و تنها با استفاده از کلید عمومی امضاکننده امکان‌پذیر می‌سازد

transport layer security abbr. TLS	امنیت لایهٔ ترابُرد	

قرارداد امنیتی و اصالت‌سنجشی که به‌طور گسترده در مرورگرها و در ارائهٔ خدمات وب به کارگرفته می‌شود

U

unconditional security	امنیت نامشروط	

امنیت در برابر رمزگشایی غیرمجاز با فرض اینکه تحلیلگر رمز امکانات محاسباتی نامحدود دارد

واژه بیگانه	معادل فارسی	تعریف
undeniable signature	امضای انکارناپذیر	

نوعی امضای رقمی که فرایند درستی‌سنجی آن تنها در صورت مشارکت صاحب امضا امکان‌پذیر است

universal forgery attack	حملهٔ جعل‌امضای 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

universal re-encryption mixnet	شبکهٔ مخلوط بازرمزگذاری عام	

نوعی شبکهٔ مخلوط بازرمزگذاری که در آن شمار گیرندگان بیش از یک نهاد است و در هر مرحله، عمل بازرمزگذاری هر پیام بدون نیاز به اطلاع از کلید عمومی گیرنده انجام می‌شود

unprotected proxy signature	امضای وکالتی حفاظت‌نشده	

نوعی امضای وکالتی که در آن هم وکیل و هم موکل می‌توانند امضای وکالتی معتبر تولید کنند، اما نهاد دیگری که توسط امضاکنندهٔ اصلی به عنوان امضاکنندهٔ وکالتی مشخص نشده باشد، چنین امکانی ندارد

V

verifiable secret sharing scheme	طرح تسهیم راز وارسی‌پذیر	

نوعی طرح تسهیم راز که در آن شرکت‌کنندگان پیش از بازیابی راز قادر به بررسی اعتبار سهم خود از راز هستند

verifier	وارسی‌کننده، وارس	

هستاری که هویت ادعایی هستار دیگر را با استفاده از یک قرارداد احراز اصالت (authentication protocol) بررسی می‌کند

verifier impersonation attack	حملهٔ جعل هویت وارسی‌کننده، حملهٔ جعل هویت وارس	

حمله‌ای که در آن مهاجم هویت وارسی‌کننده را در یک قرارداد احراز اصالت (authentication protocol) جعل می‌کند

واژه بیگانه	معادل فارسی	تعریف
vernam cipher syn. one-time pad cipher	رمز یکبار مصرف	رمزی که در آن از کلید رمز تنها یک بار استفاده می‌شود به‌طوری‌که هر حرف یا نماد کلید برای رمز کردن یک نماد متن اصلی به کار می‌رود
video steganography	نهان‌نگاری تصویرمتحرک	ارسال پیام محرمانه با استفاده از داده‌های ویدیویی به‌عنوان رسانهٔ پوششی
visual attack	حملهٔ دیداری	آزمودن دیداری تصاویر نهانه به‌منظور پیداکردن تفاوت بین نهانهٔ تصویری و پوشانهٔ تصویری (میزبان) متناظر با آن‌ها
visual cryptography	رمزنگاری دیداری	رمزنگاری اطلاعات بصری، اعم از تصویر و متن و جز آن، که برای رمزگشایی از آنها دستگاه بینایی انسان کفایت می‌کند و به رایانه نیازی نیست
visual secret sharing scheme	طرح تسهیم راز دیداری	نوعی طرح تسهیم راز که در آن شرکت‌کنندگان ازطریق ابزارهای دیداری قادر به بازیابی راز هستند
voice scrambling	درهم‌ریزی صدا	یکی از راه‌های رمزکردن نشانک‌ها/ سیگنال‌های گفتار(صدا) که با تغییردادن وابستگی‌های زمانی و دامنه و بسامد انجام می‌شود و نباید تأثیر قابل‌توجهی در پهنای باند نشانک/ سیگنال داشته باشد
vulnerability scanner syn. port scanner	پویشگر آسیب‌پذیری مت. پویشگر درگاه	برنامه‌ای رایانه‌ای که برای ارزیابی ضعف‌های امنیتی سامانه‌های رایانه‌ای و شبکه‌ها و برنامه‌های کاربردی یا نرم‌افزاری طراحی شده است

واژه بیگانه	معادل فارسی	تعریف

W

watermark — تەنقش

داده‌های حامل شناسانه‌های منابع یا مالکان اثر و احتمالاً اطلاعات اختیاری دیگر

watermarking — تەنقش‌گذاری

روشی در امنیت رایانه‌ای مبتنی بر گنجاندن شناسانه‌های منابع یا مالکان آثارِ آنالوگ یا رقمی در داخل منبع به‌منظور 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 به‌طوری‌که:

$$hash(m_1) = hash(m_2)$$

دشوار باشد

Weak physical unclonable function
abbr. weak PUF — تابع فیزیکی تکثیرناپذیر ضعیف
مت. تفت ضعیف

نوعی تابع فیزیکی تکثیرناپذیر با تعداد بسیار محدودِ چالش و دسترسی واپایش‌شدهٔ مهاجم به آن

wiretapping — شنود خط، خط‌شنود

کسب اطلاعات ازطریق اتصال به یک سیم یا سایر رساناهایی که برای ارتباطات به کار گرفته می‌شوند

Z

zeroization — صفرسازی

روشی برای پاک کردن داده‌ها و کلیدهای رمزنگاشتی و اعتبارنامه‌هایی که به‌صورت الکترونیکی ذخیره شده‌اند، ازطریق تغییر یا حذف محتوای داده‌های ذخیره‌شده با هدف جلوگیری از بازیابی آنها

واژه بیگانه	معادل فارسی	تعریف
zero-knowledge proof	اثبات ناتراوا، اثبات دانش‌صفر	نوعی روش اثبات در رمزنگاری که در آن اثبات‌کننده می‌تواند به وارسی‌کننده اثبات کند که یک گزارهٔ مفروض درست است، بدون آنکه هیچ اطلاعاتی به‌جز درستی گزاره به وارسی‌کننده منتقل شود
zero-knowledge property abbr. ZK proof	ویژگی ناتراوایی، ویژگی دانش‌صفری	خصوصیتی که به اثبات‌های تعاملی و استدلال‌های تعاملی و غیرتعاملی نسبت داده می‌شود و خواستهٔ اثبات‌کننده مبنی بر عدم نشت اطلاعات در طرح‌های اثبات ناتراوا را تأمین می‌کند
μ		
μ-memory leakage resilient protocol abbr. μ-MLR protocol	قرارداد پارنشت‌تاب حافظه اختصار: قرارداد پارنشتاب	قراردادی که حتی با آشکار شدن بخشی (μ درصد) از اطلاعات سرّی ذخیره شده در حافظه، امن باقی بماند
μ-non-volatile memory attacker abbr. μ-NVM attacker	مهاجم پارآگاه از حافظهٔ غیرفرّار اختصار: مهاجم پارآگاه	حمله‌وری که قادر به دستیابی به بخشی (μ درصد) از اطلاعات سرّی ذخیره شده در حافظهٔ غیرفرّار باشد

واژه‌های مشترک

واژه بیگانه	واژه مصوب	حوزه	تعریف
A			
access control	واپایش دسترسی	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	فرایندی امنیتی که در آن از منابع مشترک در برابر دسترسی غیرمجاز محافظت می‌شود نظارت خودکار یا دستی بر دسترسی به خدمات خاص یا بخش معینی از شبکه
access level	سطح دسترسی	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	سلسله‌مراتب ناظر بر سطح امنیت که برای تعیین میزان حساسیت داده‌های سامانهٔ اطلاعات و صدور یا عدم صدور مجوز دسترسی کاربران به کار می‌رود
access protection	حفاظت دسترسی	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	فرایند حفاظت از حلقهٔ محلی در برابر خرابی‌ها یا ازکارافتادن‌های (outages) شبکه که به شکل‌های مختلف انجام می‌شود، ازجمله تهیهٔ دو مکان برای استقرار تأسیسات محلی و افزودن کلیدهای محافظ به سرهای حلقه‌های محلی
accumulator	انباشتگر	رایانه و فنّاوری اطلاعات، رمزشناسی	ثبّاتی که نتایج عملیات انجام‌شده در واحد حساب و منطق را در خود نگه می‌دارد
active attack	حملهٔ فعال	رایانه و فنّاوری اطلاعات، رمزشناسی	ورود بدون اجازه به شبکهٔ رایانه‌ای، همراه با حذف یا تغییر داده‌های ذخیره‌شده در آن
add-on security	برافزایی امنیت	رمزشناسی، مهندسی مخابرات	تقویت سازوکارهای حفاظت ازطریق افزایش امکانات نرم‌افزاری یا سخت‌افزاری که پس از رسیدنِ سامانه به بهره‌برداری انجام می‌شود
adequate security	امنیت کافی	رمزشناسی، مهندسی مخابرات	امنیت متناسب با خطر و آسیب ناشی از تخریب یا سوءاستفاده یا دست‌کاری یا دسترسی غیرمجاز به اطلاعات
B			
baseline security	امنیت پایه	رمزشناسی، مهندسی مخابرات	معیارهای امنیتی موفقی که الگویی برای اجرا در سازمان‌های مشابه قرار می‌گیرند

واژه بیگانه	واژه مصوب	حوزه	تعریف
biometric	زیست‌سنجشی	رایانه و فنّاوری اطلاعات، رمزشناسی	مربوط به زیست‌سنجی
biometrics 1	زیست‌سنجه	رایانه و فنّاوری اطلاعات، رمزشناسی	هر خصوصیت زیستی یا فیزیکی که با رایانه قابل اندازه‌گیری و بازشناسی خودکار باشد
biometrics 2	زیست‌سنجی	رایانه و فنّاوری اطلاعات، رمزشناسی	۱. مطالعهٔ زیستیِ قابل اندازه‌گیری با رایانه ۲. در امنیت رایانه، مجموعهٔ فنون اصالت‌سنجی مبتنی بر آن دسته از خصوصیات فیزیکیِ قابل‌اندازه‌گیری که به‌طور خودکار بازشناسی می‌شود
bit	بیت	رایانه و فنّاوری اطلاعات، رمزشناسی	رقم دوگانی صفر یا یک

C

cascade	آبشاره	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	سلسله‌فعالیت‌های پیوسته در پردازش داده‌ها که در آن انجام هر مرحله وابسته به وقوع مرحلهٔ قبل است
coding	کُدگذاری	رایانه و فنّاوری اطلاعات، رمزشناسی	وضع قواعدی برای انطباق عناصری از یک مجموعه بر عناصری از مجموعهٔ دیگر و معمولاً با تناظر یک‌به‌یک
common criteria	ضوابط عام	رمزشناسی، مهندسی مخابرات	ضوابطی جامع و سخت‌گیرانه برای تعیین کارایی امنیتی و حصول اطمینان از عملکرد سامانه‌ها و محصولات
common criteria for information technology security	ضوابط عام برای امنیت فنّاوری اطلاعات	رمزشناسی، مهندسی مخابرات	استانداردی برای ارزیابی سامانه‌ها و محصولات فنّاوری اطلاعات از قبیل سامانهٔ عامل و شبکه‌های رایانه‌ای و سامانه‌های گسترده و برنامه‌های کاربردی

واژه بیگانه	واژه مصوب	حوزه	تعریف
computer fraud	تقلب رایانه‌ای	رایانه و فنّاوری اطلاعات، رمزشناسی	هرنوع دستکاری در سامانه‌های رایانه‌ای برای سوءاستفاده یا فریبکاری
cryptography	رمزنگاری	رایانه و فنّاوری اطلاعات، رمزشناسی	تبدیل یک متن آشکار به متنی رمزی‌شده با استفاده از کلید به‌منظور حفاظت از داده‌های مهم در برابر مهاجمان و تأمین محرمانگی یا یکپارچگی یا احراز اصالت پیام یا شناسایی یک هستار
cryptological	رمزشناختی	رایانه و فنّاوری اطلاعات، رمزشناسی	مربوط به رمزشناسی
cryptologist	رمزشناس	رایانه و فنّاوری اطلاعات، رمزشناسی	متخصص علم رمزشناسی
cybercrime	جُرم رایانه‌ای	رایانه و فنّاوری اطلاعات، رمزشناسی	جُرمی که با استفاده از رایانه یا شبکهٔ اینترنتی انجام می‌شود

D

واژه بیگانه	واژه مصوب	حوزه	تعریف
data	داده مت. داده‌ها	باستان‌شناسی، رایانه و فنّاوری اطلاعات، رمزشناسی	[باستان‌شناسی] اطلاعات کمّی حاصل از مشاهدهٔ یافته‌ها که مبنای استدلال و بحث و محاسبه قرار می‌گیرد [رایانه و فنّاوری اطلاعات، رمزشناسی] اعداد و متن و مانند آن که می‌توان آنها را به شکل خاصی مرتب کرد تا امکان ذخیره‌سازی و پردازش آنها به‌وسیلهٔ رایانه فراهم شود
data analysis	تحلیل داده‌ها	آمار، رایانه و فنّاوری اطلاعات، رمزشناسی	[آمار] فرایندی با هدف استخراج اطلاعات مفید که معمولاً مشتمل است بر پالایش و انتقال و مدل‌بندی داده‌ها [رمزشناسی، رایانه و فنّاوری اطلاعات] فرایند به کار بستن سامانمند روش‌ها و فنون آماری و منطقی برای توصیف و خلاصه‌سازی و مقایسهٔ داده‌ها

تعریف	حوزه	واژه مصوب	واژه بیگانه
	رایانه و فنّاوری اطلاعات، رمزشناسی	حفاظت داده‌ها	data protection

محافظت از اطلاعات سامانه در برابر دستیابی غیرمُجاز به داده‌ها و تغییر عمدی یا سهوی آنها به دلیل خطاهای کاربری و خرابی‌های رایانه‌ای

E

	رایانه و فنّاوری اطلاعات، رمزشناسی	کارایی	efficiency

میزان عملکرد مناسب نرم‌افزار با توجه به منابع به‌کارگرفته‌شده در شرایط معین

	رایانه و فنّاوری اطلاعات، رمزشناسی	کارا	efficient

سخت‌افزار یا نرم‌افزار، الگوریتم یا طرحی که کارایی داشته باشد

	رایانه و فنّاوری اطلاعات، رمزشناسی	دولت الکترونیکی	e-government, digital government, online government, internet-based government

استفادهٔ دولت از فناوری اطلاعات برای مبادلهٔ اطلاعات و خدمات با شهروندان و بخش خصوصی و سایر نهادها

	رایانه و فنّاوری اطلاعات، رمزشناسی	ای ـ باجه مت. باجهٔ الکترونیکی	e-kiosk syn. electronic kiosk

نوعی دستگاه الکترونیکی برای دسترسی به اطلاعات که در مکان‌های عمومی نصب می‌شود

	رایانه و فناوری اطلاعات، رمزشناسی	چک الکترونیکی متـ. ای ـ چک	electronic cheque syn. e-cheque

انتقال وجه به‌صورت الکترونیکی ازطریق برداشت مستقیم پول از حساب الکترونیکی فرد

	رایانه و فناوری اطلاعات، رمزشناسی	تجارت الکترونیکی	electronic commerce syn. e-commerce

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

تعریف	حوزه	واژه مصوب	واژه بیگانه
	رایانه و فناوری اطلاعات، رمزشناسی	پول الکترونیکی متـ. ای ـ پول	electronic money syn. electronic cash syn. cybermoney syn. cybercash syn. digicash syn. digital money syn. digital cash syn. e-money syn. e-cash

پولی که ازطریق اینترنت ردوبدل می‌شود

	رایانه و فناوری اطلاعات، رمزشناسی	پرداخت الکترونیکی متـ. ای‌ـ پرداخت	electronic payment syn. e-payment

پرداخت وجه به‌صورت الکترونیکی

	اقتصاد، رایانه و فناوری اطلاعات، رمزشناسی	امضای الکترونیکی	electronic signature syn. e-signature

[اقتصاد] پروندهٔ رقمی که همراه با قرارداد یا به پیوست آن است و ازنظر 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

	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات	متن رمزگذاری‌شده	encrypted text

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

	رایانه و فناوری اطلاعات، رمزشناسی	امنیت الکترونیکی متـ. ای ـ امنیت	electronic security syn. e-security

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

	رایانه و فناوری اطلاعات، رمزشناسی	خدمات الکترونیکی متـ. ای ـ خدمات	electronic services syn. e-services

خدماتی که ازطریق اینترنت عرضه می‌شود

واژه بیگانه	واژه مصوب	حوزه	تعریف

F

feedback	بازخورد	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	بازگرداندن بخشی از نشانک/ سیگنال خروجی افزاره به ورودی آن

I

implementation	پیاده‌سازی	رایانه و فنّاوری 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 اطلاعاتی	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 فنّاوری اطلاعات، ، رمزشناسی، علوم کتابداری و اطلاع‌رسانی	محافظت از سامانه‌های اطلاعاتی در مقابل دسترسی‌های غیرمجاز یا دستکاری اطلاعات در مرحلهٔ ذخیره‌سازی یا پردازش یا انتقال
infrastructure	زیرساخت	حمل‌ونقل درون‌شهری-جاده‌ای، رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	[رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات] مجموعهٔ عناصر پایه‌ای برای انجام یک فعالیت یا ایجاد یک سامانه [حمل‌ونقل درون‌شهری-جاده‌ای] تمام اجزای ثابت سامانه‌های حمل‌ونقل مانند حریم راه، خطوط مسیر، تجهیزات علامت‌دهی، ایستگاه‌ها، محوطه‌های پیاده ـ سوار، ایستگاه‌های اتوبوس و امکانات نگهداری

تعریف	حوزه	واژه مصوب	واژه بیگانه

K

	رایانه و فنّاوری اطلاعات، رمزشناسی	کلید	key

[رایانه و فنّاوری اطلاعات، رمز] مقداری که از آن برای واپایش عملیات رمزنگاشتی مانند رمزگشایی و رمزگذاری و امضا یا وارسی آن، استفاده می‌کنند

M

	رایانه و فناوری اطلاعات، رمزشناسی	بدافزار	malware syn. malicious ware

نرم‌افزاری که برای تسلط بر سامانهٔ 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 به‌صورت پودمان‌های مختلف طراحی شده باشد

	رایانه و فنّاوری 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 ازطریق نمایشگر

N

	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات	شبکه	network

مجموعه‌ای از گره‌های ارتباطی که ازطریق مجراهایی به هم متصل‌اند

O

	رایانه و فناوری اطلاعات، رمزشناسی	برون‌خط	off-line

تعریف	حوزه	واژه مصوب	واژه بیگانه
وضعیت قطع ارتباط از رایانهٔ مرکزی			
	رایانه و فناوری اطلاعات، رمزشناسی	برخط	on-line
وضعیت یا حالت وصل بودن به رایانهٔ مرکزی			

P

	رمزشناسی، مهندسی مخابرات	امنیت فیزیکی	physical security
جلوگیری از دسترسی فیزیکی غیرمجاز به سامانه‌ها			
	رایانه و فناوری اطلاعات، رمزشناسی	پردازنده	processor
واحدی در رایانه که تفسیر و اجرای دستورالعمل‌ها را بر عهده دارد			
	رایانه و فناوری اطلاعات، رمزشناسی	داده‌های حفاظت‌شده	protected data
اطلاعاتی در یک سامانه که در برابر دستیابی غیرمُجاز به داده‌ها و تغییر عمدی یا سهوی آنها به‌طور ناخواسته یا به دلیل خطاهای کاربری و خرابی‌های رایانه‌ای محافظت شده باشد			
	رایانه و فناوری اطلاعات	کلید عمومی	public key
یکی از دو کلید ویژهٔ "رمزگذاری با کلید عمومی" که در اختیار کسانی قرار می‌گیرد که می‌خواهند پیام رمزشده بفرستند			
	رایانه و فناوری اطلاعات	رمزگذاری با کلید عمومی	public key encryption
نوعی رمزگذاری که در آن از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود			

Q

	رایانه و فناوری اطلاعات، رمزشناسی	پُرسمان	query
درخواست اطلاعات از یک دادگان			

R

	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات	اطمینان‌پذیر متـ. قابل اطمینان	reliable
ویژگی سامانه‌ای که دارای اطمینان‌پذیری یا قابلیت اطمینان است			

واژه بیگانه	واژه مصوب	حوزه	تعریف
reliability	اطمینان‌پذیری متـ. قابلیت اطمینان	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات	

میزان توانایی یک سامانهٔ نرم‌افزاری برای ارائه عملکردی معین در دورهٔ زمانی و شرایط مشخص

redundancy	افزونگی	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات	

بخشی از هر پیام که برای افزایش اطمینان یا ستبری (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	

شنود 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	

واکاوی 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 خط‌ِمشی امنیتی آن سامانه شود