مجموعه واژه‌های مصوب

گروه واژه گزینی انجمن رمز ایران

(کارگروه واژه‌گزینی رمزشناسی فرهنگستان)

در فرهنگستان زبان و ادب فارسی

شهریورماه ۱۴۰۲

به نام خدا

پیش‌گفتار

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

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

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

جواد مهاجری

شهریور ۱۴۰۲

واژه‌های مصوب

واژه بیگانه	معادل فارسی	تعریف

A

access control — واپایش دسترسی

فرایندی امنیتی که در آن از منابع مشترک در برابر دسترسی غیرمجاز محافظت می‌شود.

accountability — 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 آزمون¬های دارای عمق نفوذ بیشتر در قیاس با آزمون‌های نفوذ غیرفعال، با بهره‌گیری از ضعف‌های امنیتی ذاتی موجود در فنّاوری 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 رمزبندی 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/ زیرساخت محاسباتی یا تخریب درستی داده‌ها یا سرقت اطلاعات موردواپایش 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 $f+1$ 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
anonymizer	گمنام‌ساز	ابزاری که ردگیری فعالیت‌ها را در اینترنت ناممکن می‌سازد.
arbiter PUF	تابع فیزیکی تکثیرناپذیر انتخاب‌گر / تفت انتخاب‌گر	نوعی تابع فیزیکی تکثیرناپذیر که بر اساس تفاوت ذاتی زمان‌بندی دو مسیر متقارن منتهی به یک بیت خروجی مدار عمل می‌کند.
asymmetric cryptography syn. public-key cryptography	رمزنگاری نامتقارن مت.رمزنگاری با کلید عمومی	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 تولید امضای دیجیتال) ایجاد می‌کند و هر هستار کدگشا که به کلید عمومی متناظر دسترسی داشته باشد می‌تواند ته‌نقش مربوط را آشکار و بازشناسی کند.
asymptotic security	امنیت مجانبی	نوعی امنیت برای یک طرح رمزنگاشتی که در آن احتمال موفقیت هر مهاجم زمان‌چندجمله‌ای احتمالاتی برای شکستن طرح در بهترین حالت ناچیز باشد؛ مجانبی بودن امنیت به‌دلیل وابستگی امنیت به رفتار طرح برای مقادیری از پارامتر امنیتی است که به اندازه 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.
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

واژه بیگانه	معادل فارسی	تعریف
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 یک کاربر به داده‌ها و سامانه‌ها و خدمات را تعیین می‌کند.

attribute-based encryption	رمزگذاری ویژگی‌بنیاد

نوعی رمزگذاری با این هدف که تنها افرادی که حائز شرایط یا ویژگی‌های خاصی هستند، قادر به رمزگشایی متن رمز باشند.

attributes authority	مرجع تأیید ویژگی

هستاری رسمی با اختیار وارسی ویژگی‌های منتسب به یک هویت

attributes management	مدیریت ویژگی‌ها

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

audio steganography	نهان‌نگاری صوتی

جا دادن پیغام محرمانه در نشانک‌های صوتی رقمی

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

واژه بیگانه	معادل فارسی	تعریف
authenticated encryption (AE)	رمزگذاری احرازاصالت‌شده مت. رمزگذاری اصالت‌سنجی‌شده	راهکاری جدید برای تأمین همزمان محرمانگی و احراز اصالت که در مقایسه با راهکار گذشته، که حاصل ترکیب مستقیم روش‌های رمزگذاری و احراز اصالت بود، بسیار سریع‌تر و کاراتر است.
authenticated encryption with associated data (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 بکارگیری رمز قالبی که به اطمینان از اصالت و یکپارچگی داده‌ها منجر می‌شود.
authentication period	دورهٔ احراز اصالت مت. دورهٔ اصالت‌سنجی	بیشینه‌زمان قابل قبول بین فرایند احراز اصالت اولیه و فرایندهای احراز اصالت بعدی، در طی زمان یک نشست واحد یا در طی زمانی که دسترسی به داده‌ها امکان‌پذیر است.

واژه بیگانه	معادل فارسی	تعریف
authentication provider	نشان‌بخش اصالت	نهادی که مسئولیت احراز اصالت اولیهٔ یک هستار و تخصیص یک نمودافزار را، که نشان‌دهندهٔ انجام احراز اصالت اولیه است، بر عهده دارد.
authentication tag	برچسب احراز اصالت مت. برچسب اصالت‌سنجی	رشته‌ای از بیت‌های متناظر با یک داده، برای تضمین اصالت آن داده
authenticator	اصالت‌نشان	ابزاری برای تأیید هویت یک کاربر یا فرایند یا افزاره
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	مجازشناسی	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.
authorization architecture	معماری مجازشناسی	مجموعه‌ای از مؤلفه‌ها و داده‌ها که اخذ و اجرای تصمیمات مجازشناسی را ممکن می‌سازد.
authorization boundary	محدودهٔ مجازشناسی	همهٔ مؤلفه‌های یک سامانهٔ اطلاعاتی که یک مقام مجازشناسی می‌تواند آنها را مجاز سازد، بی‌آن‌که سایر سامانه‌های مجاز متصل به آن را در بر گیرند.

واژه بیگانه	معادل فارسی	تعریف
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 یک 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.

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.

واژه بیگانه	معادل فارسی	تعریف
balance property	ویژگی توازن	

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

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	مسئلهٔ دیفی ـ هلمن دوخطی	

مسئله محاسبه $\hat{e}\ (p,p)^{abc}$ 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]	

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

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.

واژه بیگانه	معادل فارسی	تعریف
bit commitment scheme	طرح تعهد بیتی	
		نوعی طرح تعهد که در آن x تنها از یک بیت تشکیل می‌شود.
bit independence criterion	معیار استقلال بیتی	
		معیاری که به‌موجب آن، تغییر هر بیت ورودی در توابع بولی به تغییر هر دو بیت خروجی دلخواه، به‌طور مستقل از یکدیگر، منجر می‌شود.
blind proxy signature	امضای وکالتی کور	
		امضایی که در آن 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.
branch number	عدد انشعاب	
		عددی که به‌عنوان معیاری برای سنجش قدرت پخش یک نگاشت به کار می‌رود.

واژه بیگانه	معادل فارسی	تعریف
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

certificate authority syn. certification authority, 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, 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	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.

واژه بیگانه	معادل فارسی	تعریف

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 طرفین قرارداد که در حین اجرای قرارداد دروغ می‌گوید یا از آن قرارداد پیروی نمی‌کند.

chosen ciphertext attack حمله با متن رمز منتخب

حمله‌ای (تحلیل رمز) که در آن مهاجم قادر به انتخاب متن‌های رمز و 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 رمز) 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 جستجو، سعی در دستیابی به کلید دارد.

واژه بیگانه	معادل فارسی	تعریف
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.

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 می‌کنند.

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.

واژه بیگانه	معادل فارسی	تعریف
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.
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 به‌دست 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 (کتاب‌کد) دسترسی دارد و بدون دانستن کلید مخفی از آنها برای رمزگشایی پاره‌ای از ارتباطات بعدی کمک می‌گیرد.
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 طرفین (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 (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
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 الگوریتم‌ها/ خوارزمی‌های 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.
computer incident response center (CIRC) syn. computer incident response team, CIRT syn. cyber incident response team	مرکز رویارویی با پیشامدهای رایانه‌ای مت. گروه 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.

واژه بیگانه	معادل فارسی	تعریف
computer incident response team (CIRT), syn. computer incident response center (CIRC) syn. cyber incident response team	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.

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.

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 (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.

Controlled Cryptographic Item (CCI) Assembly	هم‌گذاری رمزاقلام واپاییده، اختصار: هم‌گذاری راو	

دستگاهی حاوی یک منطق رمزنگاشتی یا یک طرح امنیت ارتباطاتی دیگر که موردتأییدNSA (آژانس امنیت ملی امریکا) 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 (CCI) Component	مؤلفهٔ رمزاقلام واپاییده، 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 (CCI) Equipment	تجهیزات رمزاقلام واپاییده، 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.

تعریف	معادل فارسی	واژه بیگانه

حملهٔ همبستگی correlation attack

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

ایمنی از همبستگی correlation immunity

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.

شیوهٔ شمارگر
counter mode
syn. integer counter mode
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 .

اثبات ناتراوای هم‌رو
concurrent zero-knowledge proof
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.

پوشانه covertext

پیغامی که داده‌های پیغام محرمانه در داخل داده‌های آن درج می‌شود.

تحلیل رمز cryptanalysis

۱. 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.
۲. عملیات محاسباتی برای به دست آوردن کلید سامانهٔ رمز، بدون آگاهی از کلید آن، با هدف نفوذ به سامانه

تحلیل‌گر رمز cryptanalyst

فردی که تحلیل رمز می‌کند و در آن تخصص دارد.

واژه بیگانه	معادل فارسی	تعریف
cryptographic primitive	نخستینهٔ رمزنگاشتی	

الگوریتم‌ها/خوارزمی‌های رمزنگاشتی شناخته‌شده و سطح‌پایین، شامل توابع چکیده‌ساز یک‌طرفه و توابع رمزگذاری که به‌طورمعمول به‌منظور ساخت (طراحی) قراردادهای رمزنگاشتی برای سامانه‌های امنیت رایانه‌ای به‌کار می‌روند.

cryptographic protocol	قرارداد رمزنگاشتی	

یک الگوریتم/خوارزمی توزیع‌شده که به‌طور دقیق تعامل میان دو یا چند هستار را برای دسترسی به اهداف امنیتی مشخص بیان می‌کند.

crypto officer	کارشناس رمز، مسئول رمز	

فرد یا اداره‌ای برای اجرای امور رمزنگاشتی

crypto period syn. key lifetime	رمزدوره مت. طول عمر کلید	

بازه‌ای زمانی که در آن کلید رمزگزاری برای یک سامانهٔ رمز معتبر است.

cryptocurrency	رمزارز	

نوعی ارز که تنها به صورت رقمی وجود دارد و برای تنظیم فرایندهای تولید، وارسی و انتقال آن به صورت مستقل از یک بانک مرکزی، از روش‌های رمزنگاشتی استفاده 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 algorithm	الگوریتم رمزنگاشتی مت. خوارزمی رمزنگاشتی	

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

واژه بیگانه	معادل فارسی	تعریف
cryptographic hash function syn. hash function syn. hashing algorithm	تابع چکیده‌ساز رمزنگاشتی مت. تابع چکیده‌ساز مت. الگوریتم چکیده‌سازی	

تابعی که طول ورودی آن دلخواه و طول خروجی آن ثابت است و از ویژگی‌های آن یک‌طرفه بودن، وابستگی خروجی به تمامی بیت‌های ورودی و بدون برخورد است.

cryptographic mode	شیوهٔ رمزنگاشتی

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

cryptographic module	پودمان رمزنگاشتی

مجموعهٔ سخت‌افزار و نرم‌افزار و ثابت‌افزار برای اجرای توابع امنیتی تأییدشده شامل الگوریتم‌ها / خوارزمی‌های رمزنگاشتی و تولید کلید

cryptographic module security policy	خط‌مشی امنیتی پودمان رمزنگاشتی

قواعد دقیق امنیتی که یک واحد رمزنگاشتی بر اساس آن عمل می‌کند.

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

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

cryptographic scheme	طرح رمزنگاشتی

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

cryptographic security	امنیت رمزنگاشتی

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

واژه بیگانه	معادل فارسی	تعریف
cryptographic strength	استحکام رمزنگاشتی	

معیاری برحسب 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

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

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	سازوکار لفاف‌بندی داده (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, DES	استاندارد رمزگذاری داده‌ها	خوارزمی/ الگوریتم مورد توافق (استاندارد) برای رمزگذاری یا رمزگشایی داده‌ها با استفاده از جدول رمز ۶۴ بیتی
data security	امنیت داده	حفاظت از داده‌ها در مقابل تغییر غیرمجاز عمدی یا تصادفی، تخریب یا افشای آن ها
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
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

واژه بیگانه	معادل فارسی	تعریف
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.

delay-based silicon PUF	تابع فیزیکی تکثیرناپذیر سیلیکونی تأخیرمبنا / تفت سیلیکونی تأخیرمبنا

دسته‌ای از توابع فیزیکی تکثیرناپذیر سیلیکونی که خروجی آن‌ها از طریق اندازه‌گیری متغیرهای تصادفی حاصل از تأخیر یک مدار رقمی/دیجیتال به‌دست می‌آید.

deniable authentication	احراز اصالت انکارپذیر مت.اصالت‌سنجی انکارپذیر

نوعی قرارداد احراز اصالت که به فرستنده امکان می‌دهد که پیامی را برای گیرنده احراز اصالت کند 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

کلید محاسبه شده توسط یک الگوریتم/ خوارزمی مشخص 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.

واژه بیگانه	معادل فارسی	تعریف

deterministic encryption رمزگذاری تعینی

نوعی خوارزمی/ الگوریتم رمزگذاری که در آن به ازای یک متن ساده و کلید مشخص فقط یک متن رمز بدست می‌آید.

dictionary attack حملهٔ واژه‌نامه‌ای

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

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 ـ خطی

نوعی حمله با متن اصلی منتخب که در دو مرحله انجام می شود. در مرحلهٔ نخست حمله، تحلیل تفاضلی و در مرحلهٔ دوم ، تحلیل خطی صورت می‌گیرد.

differential-linear attack حملهٔ تفاضلی- خطی

نوعی تحلیل با متن اصلی منتخب با راهکار 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 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 steganography نهان‌نگاری رقمی

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

واژه بیگانه	معادل فارسی	تعریف
digraph syn.: bigram	دونویسه	یک زوج مرتب متشکل از حروف (نویسه‌ها) در متن رمز
digraphic substitution syn.: bipartite substitution	جانشینی دوبخشی	نوعی جانشینی که در آن از دونگاشت‌ها برای جایگزینی دونویسه‌ها(زوج‌های مرتب از نویسه‌ها)ی متن اصلی استفاده می‌شود.
discretionary access control	واپایش دسترسی انتخابی	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 طرفین 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
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.
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.

واژه بیگانه	معادل فارسی	تعریف

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 می‌ماند.

E

eavesdropper — 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 بدین‌ترتیب، امکان تشکیل یک کتاب‌کد 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

encipher
syn. encrypt — رمزگذاری کردن

تبدیل متن اصلی به متن رمزشده با استفاده از ابزار رمزنگاشتی

enciphered
syn. encrypted — رمزگذاری‌شده، رمزیده

داده های رمزشده

واژه بیگانه	معادل فارسی	تعریف
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	فرآیند 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 سامانه رمزنگاشتی که برای اشخاص یا طرف‌های غیرمجاز مفهوم نباشد.
encryption syn. enciphering	رمزگذاری	فرآیند 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 رمزی‌شده به‌نحوی‌که 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 مبدأ تا مقصد

واژه بیگانه	معادل فارسی	تعریف
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 آن که 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
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

واژه بیگانه	معادل فارسی	تعریف
fail-stop digital 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 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 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.

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 ثبات انتقال و یک تابع بازخورد که به عنوان عنصر اصلی مولد کلید اجرایی در رمز جریانی استفاده می‌شود.

filter generator	مولد پالایه‌ای	

نوعی مولد کلید جریانی برای الگوریتم/خوارزمی‌های رمز جریانی، متشکل از یک ثاب خطی(ثبّات انتقال بازخوردی خطی) که خروجی آن از اعمال یک تابع غیرخطی بر روی برخی از حالت‌های ثبّات حاصل می‌شود.

واژه بیگانه	معادل فارسی	تعریف
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 ۲ به توان n بار اقدام، موفق به یافتن پیامی با همان مقدار چکیده شود.

first-preimage resistance syn. preimage resistance	مقاومت در برابر پیش‌تصویر اول مت. مقاومت در برابر 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.

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

بکارگیری تمام منابع محاسباتی یا ارتباطی با ارسال درخواست‌های زیاد برای اختلال در کار یک سامانه

forward secrecy	رازمانی پیش‌سو

خصوصیتی در طرح تبادل کلید که بنا بر آن لو رفتن کلید یک نشست تنها بر امنیت همان نشست تأثیر گذارد و تهدیدی برای امنیت نشست‌های پیشین نباشد.

freshness attack syn. replay attack	حمله تکرار

حمله‌ای با هدف نقض تازگی پیام، که در آن مهاجم پیامی را که در اجرای قبلی قرارداد احراز اصالت ذخیره کرده است، در اجرای جدید آن تکرار می‌کند.

full non-volatile memory attacker	مهاجم تام‌آگاه از حافظهٔ غیرفرّار

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

fully memory leakage resilient (FMLR) protocol	قرارداد تام‌نشت‌تاب حافظه

قرارداد(پروتکلی) امن در برابر نشت کامل اطلاعات از حافظهٔ غیرفرّار

تعریف	معادل فارسی	واژه بیگانه

رمزگذاری تابعی functional encryption

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.

G

ریسهٔ صفر gap

صفرهای متوالی در یک دنبالهٔ دودویی که بیت پیش و پس از آن یک باشد.

گروه گسست دیفی ـ هلمن gap Diffie-Hellman group

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

مسئلهٔ گسست دیفی ـ هلمن gap Diffie-Hellman problem

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

حملهٔ وارونی تعمیم‌یافته generalized inversion attack

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

اصالت‌نشان گروهی group authenticator

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

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

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 (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 (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 تعداد زیادی 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.
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
ID-based cryptosystem Syn. identity-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 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

واژه بیگانه	معادل فارسی	تعریف
identity registeration	ثبت شناسه	
		فرایند معرفی شناسهٔ یک شخص به سامانهٔ وارسی شناسهٔ شخصی با استفاده از یک شناسانهٔ منحصربه‌فرد متناظر
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.
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 قرارداد(پروتکل) 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 عدم انکار
information warfare	جنگ اطلاعاتی	
		عملیاتی با هدف تخریب یا دستیابی به منابع اطلاعاتی طرف مقابل(قربانی)

واژه بیگانه	معادل فارسی	تعریف
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 .

integrity check value

قدرآزمای یکپارچگی

نوعی جمع‌آزما (checksum) با قابلیت کشف تغییر در یک سامانهٔ اطلاعاتی

intractable problems

مسائل مهارناپذیر

مسائلی که در زمان چندجمله‌ای قابل‌حل نیستند، زیرا محاسبهٔ جواب آن‌ها به‌سرعت غیرعملی می‌شود.

invasive attack

حملهٔ تهاجمی

اقداماتی برای حفاظت از اطلاعات و سامانه‌های اطلاعاتی از طریق کسب اطمینان از دسترس‌پذیری، یکپارچگی، احراز اصالت (اصالت سنجی)، محرمانگی و عدم انکار

inversion attack

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 شرکت کننده در پروتکل (قرارداد) از دستیابی طرف‌های مقابل به اطلاعات سرّی یکسان برای تولید کلید

key distribution — توزیع کلید

یکی از مهم‌ترین مباحث مرتبط با سامانه‌های رمز که کلیدها را در اختیار پودمان‌ها قرار می‌دهد.

key distribution centre — مرکز توزیع کلید

هستاری که 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 (KEM) — سازوکار لفاف‌بندی کلید (سِلک)

رمزگذاری نامتقارن برای رمزگذاری یک کلید متقارن

key escrow — امان‌سپاری کلید

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

key establishment — برقراری کلید

روند توزیع امن کلیدهای رمزنگاشتی بین پودمان‌ها

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-key) از کلید رمز یا کلید اصلی (main key)		
	طول‌عمر 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 به منظور توزیع امن کلیدهای رمزنگاشتی به صورت الکترونیکی برای کاربران مجاز		
	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		
	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		
	فرانمای کلید	key schedule
الگوریتمی برای تولید زیرکلیدها در دورهای مختلف یک رمز قالبی، با استفاده از کلید منتخب کاربر		

واژه بیگانه	معادل فارسی	تعریف
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 آن ها

knapsack problem — مسئلهٔ کوله‌پشتی

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

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 زوج‌های پیام–امضا (message-signature pairs) صورت می گیرد.

واژه بیگانه	معادل فارسی	تعریف
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.

L

lattice-based cryptography	رمزنگاری مشبکه‌بنیاد	

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

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

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 پنهان کردن اطلاعات با استفاده از روش‌ها و قواعد زبانی

واژه بیگانه	معادل فارسی	تعریف
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 داده ها از جمله داده های مسیریابی، انجام عملیات رمزگشائی برای ادامه مسیر، در مسیریاب ها ضروری است.
logical attack	حملهٔ منطقی	حمله‌ای با هدف بازیابی داده‌های سرّی از تجهیزات امن بدون آسیب‌رسانی جدی به آنها

M

malleability	چکش‌پذیری	خاصیت یک خوارزمی/ الگوریتم که به‌موجب آن با داشتن متن رمزشدهٔ c1، تولید یک متن رمزشدهٔ دیگر مانند c2، با ارتباط معلوم بین متن‌های اصلی متناظر آنها امکان‌پذیر باشد.
mandatory access control	واپایش دسترسی اجباری	نوعی واپایش برای محدود سازی دسترسی به منابع، توسط مدیر شبکه براساس مجموعه‌ای از قوانین و مقررات الزامی
man-in-the-middle attack	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 دو طرف 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.

تعریف	معادل فارسی	واژه بیگانه
	اثبات بیش‌تراوا مت. اثبات بیشینه‌افشا	maximum disclosure proof

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.

	حملهٔ تلاقی‌درمیان	meet-in-the-middle attack

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.

	تابع فیزیکی تکثیرناپذیر سیلیکونی حافظه‌مبنا مت. تفت سیلیکونی حافظه‌مبنا	memory-based silicon PUF

دسته‌ای از توابع فیزیکی تکثیرناپذیر سیلیکونی که خروجی آن‌ها از طریق اندازه‌گیری تغییرات آن مشخصه‌های تصادفی که بین افزاره‌های سیلیکونی مشابه در عناصر حافظه‌های دوحالتی وجود دارد به دست می‌آید.

	کد احراز اصالت پیام، کد اصالت‌سنجی پیام (کاپ)	message authentication code (MAC)

نوعی جمع‌آزمای رمزنگاشتی مبتنی بر رمزنگاری متقارن برای کشف تغییرات رخ-داده بر روی داده‌ها، اعم از عمدی یا تصادفی

	چکیده‌پیام	message digest

نسخهٔ فشرده‌شدهٔ یک پیام اصلی که با استفاده از خوارزمی/ الگوریتم چکیده‌ساز تولید می‌شود.

	اثبات کم‌تراوا مت. اثبات کمینه‌افشا	minimum disclosure proof

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.

	حملهٔ بازتابی	mirror attack syn. reflection attack

نوعی حملهٔ تکرار که در آن مهاجم با قطع ارتباط، پیام ارسالی توسط یکی از دو طرف ارتباط را به خود او باز می‌گرداند.

واژه بیگانه	معادل فارسی	تعریف
miss in the middle attack	حملهٔ بی‌تلاقی درمیان	

روشی برای یافتن تفاضل‌های ناممکن در خوارزمی/ الگوریتم رمز که ایده آن یافتن زوج‌متن‌هایی است که نتایج میانی حاصل از اعمال فرایند خوارزمی‌ها/ الگوریتم‌های رمزگذاری و رمزگشایی بر روی آن‌ها با هم مطابقت ندارند.

mix network syn. mixnet	شبکهٔ مخلوط	

سامانه‌ای برای گمنام‌سازی فرستندگان پیام با استفاده از عملیات رمزنگاشتی و جای‌گشتی در چند مرحله

mixnet Syn.mix network	شبکهٔ مخلوط	سامانه‌ای برای گمنام‌سازی

سامانه‌ای برای گمنام‌سازی فرستندگان پیام با استفاده از عملیات رمزنگاشتی و جای‌گشتی در چند مرحله

monoalphabetic cipher, monoalphabetic substitution cipher syn. simple substitution cipher	رمز جانشینی ساده	

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

m-resilient	m-تابا	

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

mth order correlation-immune Boolean function	تابع بولی همبستگی‌ایمن 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.

واژه بیگانه	معادل فارسی	تعریف
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.

multisignature	چندامضایی	

نوعی امضای آستانه‌ای که در آن گمنامی امضاکنندگان حفظ نمی‌شود.

multivariate public key cryptosystem	سامانهٔ رمزکلید عمومی چندمتغیره	

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

N

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

نوعی ثبّات انتقال بازخوردی که تابع بازخورد آن غیرخطی است.

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

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

nonce	تک‌بار	

عدد یا رشته ای عددی که برای مقابله با حملهٔ تکرار، تنها یک بار در یک الگوریتم یا پروتکل(قرارداد) رمزنگاشتی به کار می‌رود.

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

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.

	حملهٔ غیرتهاجمی	non-invasive attack

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

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

نوعی ثبّات انتقال بازخوردی که تابع بازخورد آن غیرخطی است.

	چکش‌ناپذیری	nonmalleability

خاصیت یک خوارزمی/ الگوریتم که به‌موجب آن با داشتن متن رمزشدهٔ c1، تولید یک متن رمزشدهٔ دیگر مانند c2، با ارتباط معلوم بین متن‌های اصلی متناظر آنها امکان‌پذیر نباشد.

	امضای انتقال‌ناپذیر	non-transferable signature

نوعی امضای رقمی که تنها از طریق فرد مشخص شده توسط امضاکننده قابل وارسی است.

O

	امضای ناآگاهانه	oblivious signature

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 مجموعه پیام‌ها باشد یا یک پیام را با استفاده از یکی از کلیدهای خصوصی خود، بدون تشخیص آن کلید امضا می‌کند.

واژه بیگانه	معادل فارسی	تعریف

oblivious transfer — 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

هستاری که حق امضای خود را به هستاری دیگر به‌عنوان امضاکنندهٔ وکالتی واگذار می‌کند.

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

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

output feedback 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 $e: G_1 \times \widehat{G_2} \rightarrow G_t$ با ویژگی‌های دوخطی بودن، و ناتباهیدگی (non-degeneracy) و محاسبه‌پذیری

واژه بیگانه	معادل فارسی	تعریف

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 مجموعه‌ی از کاربران، بدون نیاز به اطلاعات سایر کاربران، تأمین می‌شود.

passive adversary مهاجم غیرفعال

مهاجمی که فقط با جست‌وجوی تمام اطلاعات قابل دسترس برخی طرف‌های قرارداد و بدون تغییر دادن آنها، سعی در فهم اطلاعات ورودی طرف‌های امین 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

passive wiretapping خط‌شنود انفعالی

پایش یا ضبط داده‌هایی که با یک خط ارتباطی ارسال می‌شوند، بی‌آنکه تغییری در آنها ایجاد شود.

penetration test آزمون نفوذ
syn.: penetration testing

نوعی روش آزمون که در آن ارزیاب‌ها با استفاده از همهٔ مستندات دردسترس (مانند طراحی سامانه، کد منبع، کتابچه‌های راهنما) و تحت محدودیت‌های خاص، سعی در دور زدن ویژگی‌های امنیتی یک سامانهٔ اطلاعاتی دارند

تعریف	معادل فارسی	واژه بیگانه
	رازمانی پیش‌سوی کامل	perfect forward secrecy

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.

	اثبات ناتراوای کامل، اثبات دانش‌صفر کامل	perfect zero-knowledge proof

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 .

	نهان‌نگاری کاملاً امن	perfectly secure steganography

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

	حملهٔ فیزیکی	physical attack

حمله‌ای به افزاره‌های رمزنگاشتی، مبتنی بر ابزارهای فیزیکی

	تابع فیزیکی تکثیرناپذیر (تفت)	physical unclonable function (PUF)

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

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

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

	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 داده های حاصل از رمزگذاری دو متن اصلی P1 و P2 با یک کلید حاصل می‌شود.

واژه بیگانه	معادل فارسی	تعریف
polyalphabetic cipher syn. polyalphabetic encryption syn.polyalphabetic substitution cipher	رمز چند الفبایی مت.رمز جانشینی چند الفبایی	نوعی رمزگذاری که در آن هر حرف متن اصلی جانشین بیش از یک حرف از الفبای رمز می‌شود و هر جانشینی با یک عنصر از کلید مشخص می‌شود.
polyalphabetic encryption syn.polyalphabetic cipher syn.polyalphabetic substitution cipher	رمز چند الفبایی مت.رمز جانشینی چند الفبایی	نوعی رمزگذاری که در آن هر حرف متن اصلی جانشین بیش از یک حرف از الفبای رمز می‌شود و هر جانشینی با یک عنصر از کلید مشخص می‌شود.
polyalphabetic substitution cipher syn.: polyalphabetic encryption syn. polyalphabetic cipher	رمز جانشینی چند الفبایی مت.رمز چند الفبایی	نوعی رمزگذاری که در آن هر حرف متن اصلی جانشین بیش از یک حرف از الفبای رمز می‌شود و هر جانشینی با یک عنصر از کلید مشخص می‌شود.
polygram substitution cipher	رمز جانشینی چندنویسه‌ای	نوعی رمز جانشینی که در آن قالب‌هایی از حروف متن اصلی جانشین قالب‌های متناظر در حروف متن رمز می‌شوند.
polygraphic substitution cipher	رمز جانشینی چندنگاره‌ای	نوعی رمزگذاری جانشینی که در آن هر حرف متن اصلی جانشین دو یا چند حرف از الفبای متن رمز می‌شود.
polynomial time algorithm	الگوریتم زمان‌چندجمله‌ای/ خوارزمی زمان‌چندجمله‌ای	الگوریتم/ خوارزمی‌ای که زمان اجرای آن تابعی چندجمله‌ای از طول ورودی آن است.
port scanner syn. vulnerability scanner	پویشگر درگاه مت.پویشگر آسیب‌پذیری	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.

power consumption attack syn. power analysis attack syn.simple power analysis 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.

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 یکین از درجهٔ m، مانند f برروی میدان F_q که $f(0) \# 0$ و مرتبهٔ آن برابر با $q^m - 1$ باشد.

primitive root	ریشه اولیه

مولد یک 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.

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

تعریف	معادل فارسی	واژه بیگانه

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 بروزرسانی دوره ای سهم ها، 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 الگوریتم احتمالاتی/خوارزمی احتمالاتی

الگوریتم/خوارزمی‌ای با قابلیت پرتاب سکه یا، به عبارت دیگر، الگوریتم/خوارزمی‌ای با دسترسی به یک منبع تصادفی برای تولید بیت‌های تصادفی نااریب که به‌طور مستقل و با احتمال ۱/۲ مقادیر ۰ یا ۱ تولید می‌کند.

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.

probabilistic polynomial time adversary مهاجم زمان‌چندجمله‌ای احتمالاتی

مهاجمی با توانایی اجرای الگوریتم‌ها/خوارزمی‌های زمان‌چندجمله‌ای احتمالاتی

واژه بیگانه	معادل فارسی	تعریف
probabilistic polynomial-time algorithm	الگوریتم زمان‌چندجمله‌ای احتمالاتی/ خوارزمی زمان‌چندجمله‌ای احتمالاتی	مهاجمی با توانایی اجرای الگوریتم‌ها/خوارزمی‌های زمان‌چندجمله‌ای احتمالاتی
probabilistic public-key encryption	رمزگذاری احتمالاتی با کلید عمومی	نوعی خوارزمی/الگوریتم رمزگذاری با کلید عمومی که در آن هر بار عمل رمزگذاری یک پیام با استفاده از یک کلید ثابت، به تولید متن‌های رمز متفاوت می‌انجامد.
processing complexity	پیچیدگی پردازشی	زمان لازم برای انجام یک حمله
product cipher syn. superencryption	رمز ترکیبی مت. اَبررمزگذاری	رمزی که از ترکیب دو یا چند تابع رمزگذاری مختلف ساخته می‌شود.
protected proxy signature	امضای وکالتی حفاظت‌شده	نوعی امضای وکالتی که در تولید کلید امضا هم وکیل و هم موکل نقش دارند؛ و 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.
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 نهاد دیگر برروی همان پیام تبدیل می‌کند؛ در حالی که این وکیل قادر به تولید امضا برروی پیام‌های دلخواه از سوی هیچ کدام از نهادها نیست.

واژه بیگانه	معادل فارسی	تعریف
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 syn.public key proxy signature	امضای وکالتی

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

proxy signer	امضاکنندهٔ وکالتی

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

pseudorandom function	تابع شبه‌تصادفی

یک تابع تعینی برحسب یک کلید و ورودی که از یک تابع واقعاً تصادفی برحسب ورودی تمایزناپذیر است.

pseudorandom number generator (PRNG)	مولد اعداد شبه‌تصادفی

مولدی که پس از مقداردهی اولیه با هر مقدار تصادفی (به‌نام 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.

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

واژه بیگانه	معادل فارسی	تعریف
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 الگوریتم/خوارزمی احتمالاتی تولید کلید و کدگذاری(درج) وکدگشایی(آشکارسازی) که در آن الگوریتم/خوارزمی تولید کلید پارامتر امنیتی را به‌عنوان ورودی دریافت و یک زوج‌کلید خصوصی و عمومی نهان‌نگاری را تولید می¬کند و الگوریتم/خوارزمی 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

quantum deniable authentication	احراز اصالت انکارپذیر کوانتومی مت.اصالت‌سنجی انکارپذیر کوانتومی	

نوعی احراز اصالت اتکارپذیر 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.

واژه بیگانه	معادل فارسی	تعریف

receiver deniable encryption — رمزگذاری گیرنده‌انکارپذیر

نوعی رمزگذاری که در آن گیرنده بتواند دریافت پیام رمزشده را انکار کند.

recipient anonymity — گمنامی گیرنده

در یک سامانهٔ پیام، عدم امکان شناسایی گیرندهٔ پیام ازطریق شنود

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 توسط 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

related key attack — حملهٔ کلید مرتبط

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

related-key cryptanalysis — تحلیل رمز کلیدمرتبط

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

relay attack — حملهٔ بازارسالی

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.

واژه بیگانه	معادل فارسی	تعریف
replay attack syn. freshness 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.

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

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.

resiliency order	مرتبهٔ تابایی	

بیشینه مقدار m که به ازای آن تابع f، m–پایدار باشد.

ring signature	امضای حلقوی	

نوعی امضای رقمی که در آن یک کاربر می‌تواند، بدون افشای نام خود، از سوی گروهی از کاربران اقدام به تولید امضا کند و برخلاف امضای گروهی، به یک نهاد مرکزی مورداعتماد نیاز ندارد.

run	ریسه	

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

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

واژه بیگانه	معادل فارسی	تعریف
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 m1 ، یافتن m2 به‌طوری‌که hash(m1) = hash(m2) 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, 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.
secure socket layer (SSL)	لایهٔ اتصال امن(لام)	قراردادی برای ایجاد ارتباط امن در اینترنت
security association	همایند امنیتی	رابطه‌ای بین دو یا چند هستار که آنها را قادر به حفاظت از داده‌هایی می‌کند که بین آنها مبادله شده است.
security specifications	مشخصات امنیتی	شرح دقیق حفاظ‌های موردنیاز برای حفاظت از یک سامانهٔ اطلاعاتی

واژه بیگانه	معادل فارسی	تعریف
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.
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 حملات 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.

واژه بیگانه	معادل فارسی	تعریف
session key	کلید نشست	کلیدی که از آن برای رمزگذاری متقارن در یک نشست استفاده و سپس آن را نابود می‌کنند.
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 طرفین 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
signature verification	درستی‌سنجی امضا مت. وارسی امضا	استفاده از یک الگوریتم/خوارزمی 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	هستاری که متن یا محتوای رقمی را امضا می‌کند.
silicon PUF	تابع فیزیکی تکثیرناپذیر سیلیکونی / تفت سیلیکونی	دسته‌ای اصلی از توابع فیزیکی تکثیرناپذیر الکترونیکی که در تراشه‌های سیلیکونی تعبیه می‌شوند.

واژه بیگانه	معادل فارسی	تعریف
simple power analysis attack syn. power analysis attack syn. power consumption attack	حمله تحلیل توانی ساده مت.حمله تحلیل توانی	

حمله‌ای که در آن مهاجم با اندازه‌گیری توان مصرفی یک ابزار رمزنگاشتی در خلال عملیات رمزنگاشتی، می‌تواند به جزئیات مشخصه‌های اصلی آن و پیاده‌سازی خوارزمی/الگوریتم رمز دست یابد.

simple substitution cipher syn.: monoalphabetic cipher, monoalphabetic substitution cipher	رمز جانشینی ساده

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

slide attack	حملهٔ لغزشی

حمله‌ای عام (attack generic) 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 الگوریتم/خوارزمی 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 در صورتی ضروری است که یک یا چند عضو به گروه بپیوندد یا آن را ترک کند، یا زوج‌کلیدهای اختصاصی یک یا چند عضو به‌روزرسانی شوند.

واژه بیگانه	معادل فارسی	تعریف
static keys	کلیدهای ایستا	کلیدهایی که طول عمر نسبتاً زیادی دارند و در تعدادی از اجراهای یک الگوریتم/خوارزمی مشترک هستند.
statistical zero-knowledge proof 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.
statistically secure steganography	نهان‌نگاری آماری‌امن	نوعی خوارزمی/ الگوریتمی نهان‌نگاری که مهاجم با قدرت محاسباتی نامحدود تنها بتواند در آن تمایز ناچیزی بین پوشانه و نهانه پیدا کند.
steganalysis	نهان‌شکنی	دانش و فن یافتن داده‌هایی که با استفاده از نهان‌نگاری پنهان شده است.
stegosystem	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	پیغامی که از درج داده‌های پیغام 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

واژه بیگانه	معادل فارسی	تعریف
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.

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 PUF	تابع فیزیکی تکثیرناپذیر قوی / تفت قوی	

نوعی تابع فیزیکی تکثیرناپذیر غیرقابل‌پیش‌بینی، با تعداد بسیار زیاد 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 (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.

تعریف	معادل فارسی	واژه بیگانه
	کوله‌پشتی اَبَرافزایشی مت. مسئلهٔ کوله‌پشتی اَبَرافزایشی	superincreasing knapsack syn. superincreasing knapsack problem

نوعی مسئلهٔ کوله پشتی که در آن اعضای مجموعهٔ اعداد صحیح، یک دنبالهٔ اَبَرافزایشی باشند.

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

نوعی مسئلهٔ کوله پشتی که در آن اعضای مجموعهٔ اعداد صحیح، یک دنبالهٔ اَبَرافزایشی باشند.

	دنبالهٔ اَبَرافزایشی	superincreasing sequence

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

	حملهٔ سی‌بل/ حملهٔ چندشناسه‌ای	Sybil attack

نوعی حمله در شبکه‌های همتابه‌همتا (peer-to-peer networks) که در آن یک گره از شبکهٔ هم‌زمان با چندین شناسه به‌طور فعال عمل می‌کند.

	رمزنگاری متقارن مت. رمزنگاری با کلید مخفی	symmetric cryptography syn. secret key cryptography, private key cryptography

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

T

	کد احراز اصالت پیام آستانه‌ای، کد اصالت‌سنجی پیام آستانه‌ای اختصار: کاپ آستانه‌ای	threshold authentication code

نوعی کد احراز اصالت پیام(کاپ) که برای تولید آن حضور حداقل تعداد مشخصی از شرکت‌کنندگان ضروری است.

	رمزنگاری آستانه‌ای	threshold cryptography

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.

تعریف	معادل فارسی	واژه بیگانه
	رمزگشایی آستانه‌ای	threshold decryption

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.

	امضای وکالتی آستانه‌ای	threshold proxy signature

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.

	امضای آستانه‌ای	threshold signature

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.

	پیچیدگی زمانی	time complexity

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

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

اگر پیچیدگی یافتن کلید برابر با K باشد، در حملهٔ بده‌بستان زمان‌ـ‌حافظه می‌توان کلید را در T مرحله (زمان) با M کلمه از حافظه به دست آورد که در آن $K = T \times M$

	حملهٔ بده‌بستان زمان ـ حافظه ـ داده	time-memory-data trade-off attack

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.

	مهرزمانی	time stamp

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

	مهرزنی زمانی	time-stamping

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.

واژه بیگانه	معادل فارسی	تعریف
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 الگوریتم‌ها/خوارزمی‌های زمان‌چندجمله‌ای در یک زمان مناسب قابل‌حل هستند.

transitive signature	امضای تراگذر، امضای ترایا	

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

transport layer security, TLS	امنیت لایهٔ ترابُرد	

قرارداد امنیتی و اصالت‌سنجی‌ای که به‌طور گسترده در مرورگرها و ارائهٔ خدمات وب کارگرفته می‌شود.

U

unconditional security	امنیت نامشروط	

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

undeniable signature	امضای انکارناپذیر	

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

واژه بیگانه	معادل فارسی	تعریف

unprotected proxy signature — امضای وکالتی حفاظت‌نشده

نوعی امضای وکالتی که 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 .

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 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.

واژه بیگانه	معادل فارسی	تعریف
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.

W

watermark — ته‌نقش

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

watermarking — ته‌نقش‌گذاری

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 m1 یافتن m2 به‌طوری‌که hash(m1) = hash(m2) دشوار باشد.

weak PUF — تابع فیزیکی تکثیرناپذیر ضعیف /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.

واژه بیگانه	معادل فارسی	تعریف
zero-knowledge property	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

واژه بیگانه	معادل فارسی	تعریف
μ-memory leakage resilient protocol	قرارداد پارنشت‌تاب حافظه	

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

واژه بیگانه	معادل فارسی	تعریف
μ-non-volatile memory attacker	مهاجم پارآگاه از حافظهٔ غیرفرّار	

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
access level	سطح دسترسی	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	نظارت خودکار یا دستی بر دسترسی به خدمات خاص یا بخش معینی از شبکه
			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	ثباتی 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

واژه بیگانه	واژه مصوب	حوزه	تعریف
adequate security	امنیت کافی	رمزشناسی، مهندسی مخابرات	امنیت متناسب با خطر و آسیب ناشی از تخریب یا سوءاستفاده یا 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
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 زیستی قابل اندازه‌گیری با رایانه ۲. در امنیت رایانه، مجموعهٔ فنون اصالت‌سنجی مبتنی بر آن دسته از خصوصیات فیزیکی 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

واژه بیگانه	واژه مصوب	حوزه	تعریف
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
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
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

واژه بیگانه	واژه مصوب	حوزه	تعریف
D			
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
data protection	حفاظت داده‌ها	رایانه و فنّاوری اطلاعات، رمزشناسی	محافظت از اطلاعات سامانه در برابر دستیابی غیرمُجاز به داده‌ها و تغییر عمدی یا سهوی آنها به دلیل خطاهای کاربری و خرابی‌های رایانه‌ای
E			
efficiency	کارایی	رایانه و فنّاوری اطلاعات، رمزشناسی	میزان عملکرد مناسب نرم‌افزار با توجه به منابع به‌کارگرفته‌شده در شرایط معین
efficient	کارا	رایانه و فنّاوری اطلاعات، رمزشناسی	سخت‌افزار یا نرم‌افزار، الگوریتم یا طرحی که کارایی داشته باشد
e-government, digital government, online government, Internet-based government	دولت الکترونیکی	رایانه و فنّاوری اطلاعات، رمزشناسی	استفادهٔ دولت از فنّاوری اطلاعات برای مبادلهٔ اطلاعات و خدمات با شهروندان و بخش خصوصی و سایر نهادها
e-kiosk syn. electronic kiosk	ای ـ باجه مت. باجهٔ الکترونیکی	رایانه و فنّاوری اطلاعات، رمزشناسی	نوعی دستگاه الکترونیکی برای دسترسی به اطلاعات که در مکان‌های عمومی نصب می‌شود

تعریف	حوزه	واژه مصوب	واژه بیگانه
	رایانه و فنّاوری 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 فنّاوری اطلاعات، رمزشناسی	تجارت الکترونیکی	electronic commerce syn.e-commerce
انجام عملیات تجاری از راه دور با استفاده از فنّاوری اینترنت و شبکه‌های رایانه‌ای			
	رایانه و فنّاوری 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 فنّاوری اطلاعات، رمزشناسی	پرداخت الکترونیکی متـ. ای‌ـ پرداخت	electronic payment syn. e-payment
پرداخت وجه به‌صورت الکترونیکی			
	اقتصاد، رایانه و فنّاوری 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 فنّاوری اطلاعات، رمزشناسی] هر نشان الکترونیکی که برای امضای اسناد یا داده‌های الکترونیکی مورد استفاده قرار می‌گیرد

واژه بیگانه	واژه مصوب	حوزه	تعریف
encrypted text	متن رمزگذاری‌شده	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	متنی که به صورتی تغییر داده شده باشد که برای اشخاص یا طرف‌های غیرمجاز مفهوم نباشد
electronic security syn. e-security	امنیت الکترونیکی متـ. ای ـامنیت	رایانه و فنّاوری اطلاعات، رمزشناسی	فرایند کسب اطمینان از محرمانه بودن و یکپارچگی و در دسترس بودن اطلاعات الکترونیکی و حفاظت از آنها
electronic services syn. e-services	خدمات الکترونیکی متـ. ای ـ خدمات	رایانه و فنّاوری اطلاعات، رمزشناسی	خدماتی که ازطریق اینترنت عرضه می‌شود
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

واژه بیگانه	واژه مصوب	حوزه	تعریف
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	[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
			[رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات] مجموعهٔ عناصر پایه‌ای برای انجام یک فعالیت یا ایجاد یک سامانه
key	کلید	رایانه و فنّاوری اطلاعات، رمزشناسی، موسیقی	[رایانه و فنّاوری اطلاعات، رمز] مقداری که از آن برای واپایش عملیات رمزنگاشتی مانند رمزگشایی و رمزگذاری و امضا یا وارسی آن، استفاده می‌کنند
			[موسیقی] در سازهای بادی چوبی، اهرمی که برای بازوبسته کردن سوراخ‌های ساز به کار می‌رود
malware Syn. malicious ware	بدافزار	رایانه و فنّاوری اطلاعات، رمزشناسی	نرم‌افزاری که برای تسلط بر سامانهٔ عامل رایانه یا آسیب رساندن به آن، بدون آگاهی یا تأیید کاربر، به کار می‌رود
mobile commerce syn. m-commerce	تجارت سیار	رمزشناسی، مهندسی مخابرات	انجام خرید یا کارهای تجاری با استفاده از تلفن‌های همراه عادی یا پیشرفته
modular	پودمانی	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	هر سامانه‌ای که به‌صورت پودمان‌های مختلف طراحی شده باشد

M

K

واژه بیگانه	واژه مصوب	حوزه	تعریف
module	پودمان	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	هر بخش از سامانه که جداگانه و مستقل از بخش‌های دیگر قابل استفاده و بهره‌برداری تحت آن سامانه باشد
monitoring	پایش	رمزشناسی، مهندسی مخابرات	نظارت بر محیط یا صحنه یا دستگاه ازطریق نمایشگر
N			
network	شبکه	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	مجموعه‌ای از گره‌های ارتباطی که ازطریق مجراهایی به هم متصل‌اند
O			
off-line	برون‌خط	رایانه و فنّاوری اطلاعات، رمزشناسی	وضعیت قطع ارتباط از رایانهٔ مرکزی
on-line	برخط	رایانه و فنّاوری اطلاعات، رمزشناسی	وضعیت یا حالت وصل بودن به رایانهٔ مرکزی
P			
physical security	امنیت فیزیکی	رمزشناسی، مهندسی مخابرات	جلوگیری از دسترسی فیزیکی غیرمجاز به سامانه‌ها
processor	پردازنده	رایانه و فنّاوری اطلاعات، رمزشناسی	واحدی در رایانه که تفسیر و اجرای دستورالعمل‌ها را بر عهده دارد
protected data	داده‌های حفاظت‌شده	رایانه و فنّاوری اطلاعات، رمزشناسی	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

واژه بیگانه	واژه مصوب	حوزه	تعریف
public key	کلید عمومی	رایانه و فنّاوری اطلاعات	

یکی از دو کلید ویژهٔ "رمزگذاری با کلید عمومی" که در اختیار کسانی قرار می‌گیرد که می‌خواهند پیام رمزبندی‌شده بفرستند

public key encryption	رمزگذاری با کلید عمومی	رایانه و فنّاوری اطلاعات	

نوعی رمزگذاری که در آن از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود

Q

query	پُرسمان	رایانه و فنّاوری اطلاعات، رمزشناسی	

درخواست اطلاعات از یک دادگان

R

reliable	اطمینان‌پذیر متـ. قابل اطمینان	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	

ویژگی سامانه‌ای که دارای اطمینان‌پذیری یا قابلیت اطمینان است

reliability	اطمینان‌پذیری متـ. قابلیت اطمینان	رایانه و فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	

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

redundancy	افزونگی	رایانه و فنّاوری 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 فنّاوری اطلاعات، رمزشناسی	

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

واژه بیگانه	واژه مصوب	حوزه	تعریف
T			
threat	تهدید	رایانه و فنّاوری 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 فنّاوری اطلاعات، رمزشناسی، مهندسی مخابرات	ضعف در طراحی و راه‌اندازی و عملکرد مدیریت یک سامانه که باعث نقض خطِ‌مشی امنیتی آن سامانه شود