به نام خدا

واژه نامه امنیت فضای تبادل اطلاعات (افتا)

نسخهٔ اول

خرداد ۱۳۸۹

کلمه	معادل فارسی	تعریف
A		
A5/1 encryption algorithm	الگوریتم رمزگذاری A5/1	الگوریتم رمز دنباله‌ای که برای رمزنگاری ارتباطات هوایی در استاندارد GSM استفاده شده است.
AAA→Authentication, Authorization, and Accounting		
abort	قطع	پایان یافتن ناگهانی و غیرطبیعی برنامه
abrogate	لغو کردن	به معنای لغو وکالت و یا بازپس‌گیری آن، مخالف لغت delegate
abstract class	ردهٔ مجرد	
abstraction	تجرید	
abuse	سوء استفاده	
academic break	شکست نظری	حمله‌ای که از لحاظ نظری موفق، ولی در عمل غیر ممکن است.
accept	قبول	
access	دسترسی، دستیابی	داشتن امکان استفاده از یک منبع اطلاعاتی
access authority	مجاز شناس دسترسی، مجوزدهنده دسترسی	مرجعی که مسئول نظارت و واگذاری حق دسترسی به افراد مجاز است.
access control	کنترل دسترسی	به توانایی در صدور مجوز دسترسی یک کاربر مشخص در یک چارچوب خاص به منابعی (مشخص) از سامانه و یا ممانعت از دسترسی وی به منابع مزبور اطلاق می شود.
access control entry (ACE)	ورودی کنترل دسترسی	
access control list (ACL)	فهرست کنترل دسترسی	فهرستی که در آن نام افراد مجاز و محدوده دسترسی آن ها به منابع سامانه مشخص شده است.
access denied	ردّ دسترسی	
access request	تقاضای دسترسی	
access restriction	محدودیت دسترسی	
access server	کارگزار دسترسی	

accessibility	دسترس‌پذیری	
account	حساب	
accountability	پاسخگویی	یک ویژگی که بر اساس آن ردگیری فعالیت‌های یک سامانه تا افراد مسئول آن امکان پذیر می شود. به این ترتیب افرادی که تخلف کرده اند و یا به امنیت سامانه حمله کرده اند، قابل شناسایی و پیگیری خواهند بود.
accounting	حسابرسی	
accredit	اعطای اعتبارنامه	
accreditation	معتبر شناختن	تصمیم یک مقام ارشد برای صدور مجوز انجام عملیات در یک سامانه اطلاعاتی و پذیرش صریح مخاطرات مرتبط بر مبنای پیاده سازی یک مجموعه کنترل‌های امنیتی مورد توافق.
accumulator	انباشتگر	ثباتی که در عملیات محاسباتی و منطقی به کار می رود و معمولا برای شمارش اقلام یا ذخیره یک حاصل جمع مورد استفاده قرار می‌گیرد.
ACE→Access Control Entry		
ACID→Atomicity, Consistency, Isolation and Durability		
acknowledgment	اعلام دریافت	
ACL→Access Control List		
acquirer	بانک فروشنده	هر پرداخت الکترونیکی معمولا شامل دو طرف است،مشتری و فروشنده. در اینجا مقصود بانک طرف فروشنده است.
acronym	سَرنام	
action	عمل	
activation data	داده‌های فعال سازی	اطلاعات محرمانه‌ای غیر از کلید، که برای دسترسی به واحدهای رمزنگاری مورد نیازند.
active attack	حملهٔ فعال	حمله‌ای که در آن دشمن محتوای پیام را تغییر دهد و یا عبور آن را متوقف کند. در مقابل حمله غیر فعال. (رجوع کنید به passive attack)
active content	محتوای فعال	محتوای فعال اشاره به دسته‌ای از مستندات الکترونیکی دارد که می توانند، بدون دخالت کاربر، منجر به انجام و یا شروع اعمال بر روی یک سکوی کامپیوتری شوند.
active misuse	سوءاستفادهٔ فعال	

active S-box	جعبهٔ جانشینی فعال	جعبه‌ای جانشینی که ورودی آن تغییر کرده باشد.
activity diagram	نمودار فعالیت	
Ad hoc network	شبکهٔ اقتضایی	شبکه‌هایی که بنا بر اقتضا برای اتصال محلی دستگاه‌هایی مانند تلفن همراه، رایانه و PDA به طور موقت تشکیل و از بین می روند.
adaptability	وفق‌پذیری	
adaptive	وفقی	
adaptive chosen ciphertext attack	حملهٔ متن رمز منتخب وفقی	یک شکل تعاملی از حمله «متن رمز منتخب» که در آن تحلیلگر تعدادی متن رمز شده را جهت رمزگشایی انتخاب می‌کند. در این حمله تحلیلگر از روی متن‌های رمزگشایی شده، متن‌های رمزشده مورد نیاز بعدی را انتخاب می کند.
adaptive chosen plaintext attack	حملهٔ متن اصلی منتخب وفقی	یک شکل تعاملی از حمله «متن اصلی منتخب» که در آن تحلیل‌گر یک سری متن اولیه را جهت رمزگذاری انتخاب می‌کند. در این حمله تحلیل‌گر از روی متن‌های رمزگذاری شده، متن‌های اولیه مورد نیاز بعدی را انتخاب می کند.
additive stream cipher	رمز دنباله‌ای جمع شونده	
address	نشانی	
address resolution protocol (ARP)	پروتکل واگشایی آدرس	
address spoofing	جعل نشانی	
adequate security	امنیت قابل قبول	امنیتی متناسب با میزان دسترسی و یا تغییر غیرمجاز اطلاعات
adjoint	الحاقی	
ADL→Architecture Description Language		
administrative	راهبری، اجرایی	
adversarial attack	حملهٔ خصمانه	
adversary	متخاصم، خصم	
adware	تبلیغ افزار	نوعی نرم افزار که اطلاعاتی درباره یک کاربر را از الگوهای مرورگر وب کاربر جمع آوری کرده، تا بر مبنای اطلاعات جمع‌آوری شده تبلیغاتی را در مرورگر وب نمایش دهد.
AE→Authenticated Encryption		
AEAD→Authenticated Encryption with Associated Data		
AES (Advanced Encryption Standard)		الگوریتم رمز قالبی از نوع جانشینی- جایگشتی که در سال ۲۰۰۱ توسط موسسه ملی استاندارد و فناوری امریکا(NIST)

		به عنوان استاندارد جدید تحت FIPS-197 جایگزین رمزDES شد. اندازه قالب داده در این رمز ۱۲۸ بیت است. تعداد دورهای الگوریتم رمز متناسب با کلیدهای به طول ۱۲۸، ۱۹۲ و ۲۵۶ بیت به ترتیب ۱۰، ۱۲ و ۱۴ دور است.
affine transformation	تبدیل مستوی	تبدیلی بین دو فضای برداری به صورت $f(x)=ax+b$
agent	عامل	
agent based	عامل مبنا	
aggregation	تجمیع، تجمع	
aggressive mode	وضعیت تهاجمی	
AH→Authentication Header		
alarm	اخطار ، اعلان خطر	
alert	هشدار	
alert correlation	همبستگی هشدارها	
algebraic attack	حملهٔ جبری	در این حمله تحلیلگر با حل دستگاه معادلات حاکم بر سیستم رمز، سعی در یافتن مقدار کلید دارد. (از آن جایی که هر سامانه رمز را می توان بر حسب دستگاه معادلاتی چند متغیره توصیف کرد، در صورتی که بتوان یک دسته جواب هم زمان برای این دستگاه معادلات پیدا کرد، در واقع سامانه رمز شکسته شده است. از جمله روش‌هایی که برای حل دستگاه معادلات چند متغیره ارائه شده است، می توان به خطی سازی، XL و الگوریتم باخ برگر(مبتنی بر یافتن پایه های گروبنر) اشاره کرد.)
algebraic degree	درجهٔ جبری	
algebraic immunity degree	درجهٔ ایمنی جبری	
algebraic normal form(ANF)	صورت نرمال جبری	هر تابع بولی $f(x_1,x_2,..,x_n)$ را می توان به صورت مجموع حاصل‌ضرب‌های متغیرهای آن نوشت. این عبارت جبری را صورت نرمال جبری f گویند. برای مثال صورت نرمال جبری یک تابع سه متغیره می تواند به صورت $f(x_1,x_2,x_3)=1+x_2+x_3+x_2x_3+x_1x_2x_3$ باشد.
algorithm	الگوریتم	مجموعه‌ای مرتب از تعدادی عمل که کار مشخصی را انجام می‌دهند. ریشه این لغت از واژه معرب «الخوارزمی» گرفته شده است. خوارزمی دانشمند ریاضیدان ایرانی متعلق به اوایل قرن سوم است.

algorithm complexity	پیچیدگی الگوریتم	
alias	نام مستعار	
alignment	هم تراز	
alignment property	خاصیت هم‌ترازی	
all-or-nothing encryption	رمزگذاری همه یا هیچ	یکی از شیوه‌های به کارگیری رمزهای قالبی که در آن امکان رمزگشایی یک بخش از پیام به تنهایی، بدون رمزگشایی کل پیام وجود ندارد.
almost perfect nonlinear function (APN)	تابع غیرخطی تقریباً کامل	
alphabet	الفبا	در رمزنگاری به مجموعه‌ای مرتب از نمادها که برای نمایش متون آشکار یا رمز شده استفاده می‌شوند ، گفته می شود.
alternating	متناوب	
alternative step generator	مولد با گام متغیر	
always trusted	همیشه معتَمد	
analytic modeling	مدل‌سازی تحلیلی	
annihilator	پوچ ساز	
anomaly detection	تشخیص ناهنجاری	
anonymity	گمنامی، ناشناسی	غیرقابل تمایز بودن یک فرد در میان دیگر افراد از یک لحاظ مشخص
anonymizers	ابزارهای گمنام ساز	ابزارهایی که به یک کاربر امکان می‌دهند تا به صورت ناشناس و بی آنکه هویتش فاش شود، در شبکه وارد و به اجرای عملیات بپردازد .
anonymous	گمنام، ناشناس	
antivirus	ضد ویروس	
applet	برنامک	
application	کاربرد	استفاده از منابع اطلاعاتی (اطلاعات و فناوری اطلاعات) در جهت پاسخگویی به یک مجموعه مشخص از نیازمندی‌های کاربران
application content filtering	پالایش محتوای کاربردی	غربال کردن محتوای برنامه کاربردی، توسط یک عامل نرم افزاری وکیل (proxy) تا ویروس‌هایی که ممکن است درون پیوست رایانامه‌ها باشد را حذف یا قرنطینه نماید، و یا گسترش های نامه اینترنتی چندمنظوره (MIME) های خاصی را مسدود نماید، و یا سایر محتواهای فعال مانند جاوا، جاوااسکریپت و کنترل های ActiveX را غربال کند.

application gateway	دروازهٔ کاربرد	
application layer	لایهٔ کاربرد	
application level firewall	حفاظ سطح کاربرد	
application programming interface (API)	واسط برنامه نویسی کاربردی	
application proxy	نمایندهٔ کاربرد	
application relay	رلهٔ کاربرد	
approved	مصوب	
arbiter	داور	
architecture description language(ADL)	زبان توصیف معماری	
archive	بایگانی	
ARP→Address Resolution Protocol		
array	آرایه	
assess	ارزیابی	
assessment method	روش ارزیابی	یک فعالیت یا عمل متمرکز توسط یک ارزیاب به منظور ارزیابی یک خصیصه امنیتی
assessment procedure	رویهٔ ارزیابی	مجموعه‌ای از فعالیت‌ها یا اعمال که توسط یک ارزیاب جهت اطمینان از امنیت یک سامانه، و عملکرد صحیح آن، و انطباق خروجی آن با نیازمندی های امنیتی سامانه، مورد استفاده قرار می گیرد.
asset	دارایی	
assignment	تخصیص	
associated data	داده- همراه، داده- پیوست	
assurance	تضمین، اطمینان	یکی از پنج هدف امنیتی، که تضمین‌های لازم جهت برقراری چهار هدف امنیتی دیگر (محرمانگی، یکپارچگی، دسترس پذیری و قابلیت حسابرسی) را در یک پیاده سازی خاص فراهم می آورد.
asymmetric cipher = two-key cipher	رمز نامتقارن= رمز دو کلیدی	یک سامانه رمز نامتقارن، سامانه‌ای شامل دو تبدیل مختلف است؛ یکی توسط کلید عمومی تعریف می شود (تبدیل عمومی) و دیگری توسط یک کلید خصوصی(تبدیل حصوصی). با این ویژگی که تعیین تبدیل خصوصی توسط تبدیل عمومی از نظر محاسباتی غیرعملی باشد.
asymptotic space complexity	پیچیدگی حافظهٔ مجانبی	مقدار حافظهٔ مورد نیاز در یک حمله مصالحه حافظه-زمان، با

		فرض نامحدود بودن زمان حمله
asymptotic time complexity	پیچیدگی زمان مجانبی	مقدار زمان مورد نیاز در یک حمله مصالحه حافظه–زمان، با فرض نامحدود بودن حافظه‌ای که در اختیار حمله کننده است.
asynchronous	ناهم‌زمان	شرایطی که در آن چند واحد نیازی به یک فرمان ساعت برای همزمانی ندارند.
atomicity	تجزیه ناپذیری	
atomicity, consistency, isolation and durability (ACID)	تجزیه ناپذیری، سازگاری، عایقی، و ماندگاری	در علوم کامپیوتر، مجموعه‌ای از ویژگی‌هاست که تضمین می کند که تراکنش پایگاه داده با اطمینان انجام گرفته است.
attach	الحاق	
attack	حمله	۱- تلاش تحلیل‌گر برای دستیابی به اطلاعاتی در مورد کلید یا متن اصلی و یا ایجاد تغییرات هدفمند بصورت پنهان. ۲- تلاشی برای نقض امنیت رایانه
attack recovery	بهبود پس از حمله، بازیابی پس از حمله	شناسایی و رفع خرابی ناشی از یک حمله در شبکه
attack signature	امضای حمله، ردپای حمله	یک مجموعه از رخدادها که وقوع و مشاهده آنها نشانگر تلاش جهت دسترسی غیرمجاز یا بروز حمله است.
attacker	مهاجم	
attribute	ویژگی	
attribute authority	مجازشناس ویژگی، مجوز دهنده ویژگی	موجودیتی که مجوز تأیید انتساب یک خصوصیت به یک هویت را دارست.
audit	ممیزی، حسابرسی	بررسی و ثبت فعالیت‌ها، جهت ارزیابی روش‌ها و ابزار کنترلی مورد استفاده در سامانه، برای تضمین انطباق آن‌ها با خط مشی های تدوین شده و ارائه پیشنهاد درباره تغییرات لازم در ابزارها، خط مشی‌ها ، یا روال های کنترلی
audit data	داده های ممیزی	ثبت فعالیت‌های سامانه به ترتیب زمانی، جهت بازسازی و بررسی رشته رخدادها، و تغییرات.
audit logic	منطق ممیزی	
audit query	پرسمان ممیزی	
audit record	سابقهٔ ممیزی، ثبت ممیزی	سوابقی که نشان می دهد چه کسانی به یک سامانه فناوری اطلاعات دسترسی داشته، و چه عملیاتی در طول مدت دسترسی خود انجام داده اند.
audit reduction tools	ابزار کاهش ممیزی	رویه‌های پیش طراحی شده جهت کاهش حجم سوابق ممیزی به منظور تسهیل بررسی غیرخودکار توسط کاربر.

audit trail	سلسلهٔ ممیزی	یک دنباله ثبت‌شده از وقایع و فعالیت‌های سامانه با حفظ ترتیب زمانی آن‌ها، به طوری که راهبر امنیتی را قادر به بازسازی فعالیت‌های گذشته سامانه کند.
auditability	قابلیت ممیزی	
authenticated encryption (AE)	رمزگذاری توام با احراز اصالت	طرح‌هایی که در آن تامین هر دو هدف محرمانگی و احراز اصالت به صورت توامان در نظر گرفته شده است.
authenticated encryption with associated data (AEAD)	رمزگذاری احراز اصالت شده با داده- همراه	طرح رمزنگاری احراز اصالت شده‌ای که همراه با داده‌های رمز نشده است. این داده‌های همراه از جمله می‌توانند سرآیند بسته‌های شبکه باشند تا مسیریاب‌ها بتوانند با خواندن آن‌ها پیام رمز شده را در مسیر درست هدایت کرده و به مقصد برسانند.
authentication	احراز اصالت	۱. تایید این که چیزی اصل و معتبر است، آن چیز می تواند هویت یک فرد و یا منشا یک پیام یا یک برنامه کامپیوتری باشد. ۲. رویه‌ای که در آن اصالت یک فرد و یا داده احراز و اثبات می‌شود. ۳. اطمینان از این که پیام دریافتی واقعاً از منبع مورد انتظار باشد. یعنی اصالت فرستنده (و پیام) برای گیرنده احراز شود.
authentication header (AH)	سرآیند احراز اصالت	
authentication server (AS)	کارگزار احراز اصالت	
authentication token	نشان احراز اصالت	اطلاعات مرتبط با احراز اصالت که در طول یک تبادل، منتقل می‌گردد.
authentication, authorization, and accounting (AAA)	احراز هویت، مجازشناسی، و حسابرسی	اصطلاحی در امنیت شبکه، برای مدلی جهت کنترل دسترسی است که در آن افراد مجاز، شناسایی و میزان دسترسی هریک از این افراد به منابع سامانه مشخص می‌شود. همچنین فعالیت این افراد در هنگام اتصال به سامانه و بهره برداری از منابع آن ثبت می گردد.
authenticity	اصالت، اعتبار	به Authentication مراجعه شود.
authority	مرجع مجاز شناس	واحدی که توانایی تصمیم گیری در مورد صدور مجوز به دیگر واحدها یا اشخاص را دارد.
authorization	صدور مجوز، مجاز شناسی	۱. صدور مجوز دسترسی به منابع، برای افرادی با ویژگی های مشخص و تحت شرایطی خاص. ۲. تصمیم اتخاذ شده توسط یک مرجع رسمی، جهت اعطا و یا عدم اعطای اجازه برای انجام یک عملیات در یک سامانه

		اطلاعاتی، براساس یک مجموعه مشخص از خط مشی های امنیتی، همراه با تقبل خطرهای احتمالی آن برای منابع، افراد، و عملیات سامانه.
authorization request	درخواست مجوز	
authorized	مجاز	
autocorrelation	خود همبستگی	میزان همبستگی یک دنباله با خودش
auto-key cipher	رمز خود کلید	رمزی که درآن برای تولید زیرکلید، از متن اصلی یا دنباله کلید اجرایی استفاده می‌شود. سیستم‌های رمز دنباله‌ای خود همزمان نمونه‌ای از این نوع رمز هستند.
automaton	خودکاره	
autonomous	خودمختار	
autonomy	خودمختاری	
availability	قابلیت دسترسی، در دسترس بودن	یکی از اهداف امنیت، به مفهوم فراهم بودن امکان استفاده از منابع یا خدمات، برای کاربران مجاز
avalanche effect	اثر بهمنی	یک ویژگی از الگوریتم‌های رمزنگاری یا توابع چکیده‌ساز که تغییر کوچکی در متن اولیه و یا کلید موجب تغییرات قابل توجهی در متن رمز شده یا خروجی تابع چکیده‌ساز می شود.(به طور متوسط موجب تغییر نیمی از عناصر دنباله خروجی شود.)
awareness	آگاهی	
B		
baby-step giant-step algorithm	الگوریتم قدم کوچک-قدم بزرگ	یک نوع الگوریتم بهبود یافته جستجوی فضای جواب برای حل مسئله لگاریتم گسسته
back door	در پشتی	۱. نقطه ضعفی که به طور عمدی در الگوریتم رمز تعبیه می-شود و یا به‌صورت تصادفی در آن وجود دارد و آگاهی از آن موجب از بین رفتن امنیت رمز، می‌شود. به عبارتی این ضعف راه را برای نفوذ به رمز برای کسی که به آن اطلاع دارد باز می‌گذارد. ۲. در پشتی ابزاری نرم افزاری است که به نفوذگر اجازه می دهد تا به یک سیستم وارد شود، بدون آن‌که به تشریفات معمول نظیر اخذ کلمه عبور و احراز هویت نیاز داشته باشد.
back up(n)	پشتیبان	
back up(v)	پشتیبان گرفتن	تهیه رونوشتی از فایل ها و برنامه ها جهت تسهیل بازیابی اطلاعات در شرایط مورد نیاز.

backbone	مازه، ستون فقرات	
backup system	سامانهٔ پشتیبانی	
backward	پس‌رو	
bacteria	باکتری	نرم‌افزاری که کاری جز تکثیر خود به صورت نمایی انجام نمی‌دهد، ولی همین امر می‌تواند موجب درگیری منابع سامانه (از جمله پردازنده، حافظه) تا سرحد نابودی شود.
bad certificate	گواهی نامعتبر	
badge	علامت، نشانه	
balance	توازن (ریاضی)، تعادل	
balanced	متوازن (ریاضی)، متعادل	یک تابع بولی متوازن نامیده می‌شود اگر تعداد دفعاتی که خروجی آن صفر می‌شود با تعداد دفعاتی که یک می‌شود، برابر باشد.
BAN logic	منطق BAN	یکی از روش‌های تحلیل صوری پروتکل‌های امنیتی که نخستین بار در سال ۱۹۸۹ توسط Needham، Abadi، Burrows معرفی شد. توسط این روش می توان پروتکل-های احراز اصالت که دسته مهمی از پروتکل‌های امنیتی محسوب می شوند را توصیف و تحلیل کرد.
bandwidth	پهنای باند، بازهٔ فرکانسی	
base	پایه، مبنا	
baseline security	امنیتِ مبنا	حداقل امنیت لازم، جهت حفاظت از یک سامانه اطلاعاتی، براساس نیازمندی‌های آن در زمینه محرمانگی، صحت و دسترس پذیری اطلاعات.
baselining	مبنا گذاری	نظارت منابع جهت تعیین الگوی مصرف عادی، به منظور کشف انحراف های جدی
bastion host	میزبان سنگر	میزبان‌سنگرها، میزبان‌هایی هستند که معمولا به دلیل وظایف‌شان در خارج از ناحیه بی طرف(DMZ) قرار دارند، مثل کارگزاران وب و کارگزاران FTP و حفاظ‌ها، به همین دلیل در معرض انواع حملات قرار دارند و باید مستحکم سازی(hardening) شوند.
bayes' theorem	قضیهٔ بیز	رابطه‌ای بین احتمالات شرطی و مشترک به صورت P(A,B)=P(A|B)P(B)=P(B|A)P(A)
BCH code	کد BCH	دسته‌ای از کدهای دوری که چند جمله‌ای مولد آن‌ها مضرب مشترکی از چند جمله‌های کمین است. این دسته کدها توسط سه نفر به نامهای Bose، Chaundhuri،

Hocquenghem ابداع شده است و جهت کنترل (تشخیص و تصحیح) خطای کانال به‌کار گرفته می شوند.		
تابع بولی که از تمام تبدیل‌های مستوی ممکن، به یک فاصله است.(قدر مطلق تبدیل والش آن به ازای همه مقادیر ثابت است.) توابع بنت برای اولین بار در سال ۱۹۷۶معرفی شدند. این توابع در طراحی توابع جانشینی الگوریتم‌های رمز قالبی و همچنین در کدهای RM و هادامارد کاربرد بسیار دارند.	تابع بنت	bent function
۱. الگوریتمی برای تعیین پیچیدگی خطی یک دنباله متناهی و محاسبه چندجمله‌ای پس‌خورد در ثبات انتقال خطی که آن دنباله را تولید کند. ۲. یک الگوریتم تکراری برای کدگشایی کدهای BCH و RS که منتهی به بدست آوردن چند جمله ای تعیین محل وقوع خطا در دنباله دریافتی می شود.	الگوریتم برلکمپ- مسی	Berlekamp–Massey algorithm
۱. از وضعیت تعادل (یا محور صفر) خارج بودن یا خارج شدن و یا خارج کردن. ۲. در مهندسی برق اگر یک سیگنال متغیر با زمان میانگین غیر صفر داشته باشد، اصطلاحاً گوییم که دارای بایاس است. در مهندسی الکترونیک، عمل فعال سازی و تعیین نقطه کار یک ترانزیستور را بایاس کردن ترانزیستور گویند.	اریبی	bias
	اریب	biased
این نماد برای توصیف رفتار حدی یک تابع وقتی متغیر آن به سمت یک مقدار خاص یا بی‌نهایت میل می‌کند به کار می-رود.	نماد O بزرگ	big-O notation
یک به یک و پوشا	دو سویه	bijective
	دودویی	binary
فرایند منتسب نمودن دو عنصر مرتبط اطلاعاتی	انقیاد	binding
	زیست سنجه	biometrics(1)
سنجه وابسته به ویژگی‌های خاص فیزیولوژیکی یک فرد مانند اثر انگشت و طرح عنبیه و یا الگوهای رفتاری وی مانند صدا و دست‌خط که در سامانه‌های شناسایی خودکار هویت افراد مورد استفاده قرار می‌گیرد.	زیست سنجشی	biometrics(2)
یکی از حملات رمزنگاری است که درآن هدف مهاجم، یافتن دو عضو متمایز از دامنه یک تابع است، به طوری که	حملهٔ روز تولد	birthday attack

مقدار تابع به ازای آن دو عضو یکسان باشد. این حمله علیه الگوریتم‌های رمزنگاری، توابع چکیده ساز و امضای دیجیتال صورت می‌گیرد.		
یکی از لم‌های پر کاربرد در دانش رمز، دلیل استفاده از این نام، شگفتی است که با شنیدن آن در ذهن افراد پدید می آید. این تناقض‌نما بیان می دارد که در مجموعه ای متشکل ار تنها ۲۳ نفر احتمال این‌که دو نفر دارای روز تولد یکسان باشند، بیش از $\frac{1}{2}$ است.	تناقض‌نمای روز تولد، پارادوکس روز تولد	birthday paradox
خاصیتی مربوط به ورودی و خروجی S-box ها، که تغییر هر بیت ورودی باید هر دو بیت دلخواه خروجی را به صورت مستقل تغییر دهد.	معیار استقلال بیتی	bit independent criterion (BIC)
در مورد ثبات انتقال خطی با انتقال بیت به بیت، به کار برده می شود.	مبتنی بر بیت، بیت‌گرا	bit-oriented
مهاجمی که صرفاً انگیزه خراب‌کاری دارد.	سیاه کلاه	black hat
ناحیه‌ای در شبکه که داده‌های ورودی به آن دور ریخته می شوند. به عبارتی بدون این‌که فرستنده حتی مطلع شود و یا پیغامی دریافت کند، بسته ارسالی او نابود می شود.	سیاه چاله	black hole
یکی از انواع حملات منع خدمت (DoS) که با دور انداختن بسته ها، به صورت انتخابی یا کامل، انجام می‌شود. در این حمله مهاجم به جای باز ارسال کردن بسته های دریافتی آن-ها را دور می اندازد.	حملهٔ سیاه چاله، حملهٔ حذف (دورانداختن) بسته	black hole attack = packet drop attack
	خلافکار (وب)	black webber
در حمله جعبه سیاه نفوذگر با آگاهی از الگوریتم رمز و داشتن ورودی‌ها و خروجی‌های یک سامانه، و بدون آن‌که اجرای عملیات رمز برای وی قابل مشاهده و در دسترس باشد، سعی می‌کند کلید رمز را بدست آورد.	حملهٔ جعبه سیاه	black-box attack
	فهرست سیاه	blacklist
برنامه مخربی که از روش‌های گوناگون جهت انتشار استفاده می کند.	حملهٔ چندوجهی	blended attack
	رونوشت محرمانه (ر.ن.م)	blind carbon copy (BCC)
نوع خاصی از انواع امضاهای رقمی که در سال ۱۹۸۳ توسط D. Chaum معرفی شد. در این امضاء، امکان امضاگرفتن از یک شخص، روی یک پیام خاص، بدون این‌که امضاء کننده	امضای کور	blind signature

		از محتوای پیام آگاهی یابد فراهم می‌شود. از جمله کاربردهای امضای کور می‌توان به حفظ حریم خصوصی در پروتکل‌های رای‌گیری الکترونیکی و پرداخت‌های الکترونیکی اشاره کرد.
blinded message	پیام کور	
blinding	کور سازی	۱. در رمزنگاری به روشی گفته می شود که توسط آن این امکان فراهم می شود که یک نهاد قادر به ارائه یک خدمت (به عنوان مثال محاسبه یک تابع) برای یک متقاضی بدون اطلاع از ورودی واقعی یا خروجی واقعی آن (تابع) باشد. ۲. روشی برای مقابله با حملات کانال جانبی
block (1)	قالب	مجموعه ای از عناصر(حروف یا بیت) با طول مشخص که به عنوان یک واحد در نظر گرفته می‌شود.
block (2)	مسدود کردن	
block cipher	رمز قالبی	در این نوع رمز، داده‌های ورودی قبل از انجام عملیات رمز نگاری در قالب‌هایی با طول ثابت چیده می‌شوند و سپس عملیات رمزنگاری روی آنها انجام می شود. طول قالب‌های ورودی و خروجی معمولاً یکسان است. سیستم رمز قالبی را می توان یک کتاب کد بزرگ وابسته به کلید دانست که با توجه به کلید، به هر قالب ورودی یک قالب خروجی متناظر می شود. در اجرا، عملیات رمزنگاری معمولا شامل تعدادی جابجایی و جایگذاری وابسته به کلید است که به تناوب در چند دور تکرار می شود. رمزهای DES وAES نمونه‌هائی شناخته شده از رمزهای قالبی هستند.
block length=block size	طول قالب، اندازه قالب	
Bluetooth	بلوتوث	استانداردی برای یکپارچه‌سازی ارتباطات بی سیم در فواصل کوتاه مثل ارتباط تلفن‌های همراه، رایانه ها و PDA ها با یک دیگر و و یا با تلفن خانگی و یا سایر وسایل.
Blum integers	اعداد بلام	اعدادی که به صورت حاصل‌ضرب دو عدد اول متمایز p وq باشند، به طوری که $p \equiv q \equiv 3 \pmod 4$
Blum–Blum–Shub generator	مولد بلام-بلام-شاب	یکی از انواع مولد های اعداد شبه تصادفی بسیار قوی.
boomerang attack	حملهٔ بومرنگ	حمله ای علیه رمزهای قالبی مبتنی بر حمله تفاضلی.
boot sector virus	ویروس قطاع راه انداز	ویروسی که در قطاع راه‌انداز رایانه مستقر می‌شود و برنامه های اصلی راه‌اندازی را آلوده می کند.

bot	بات	مخفف Robot. برنامه‌ای است که برای انجام وظایف خودکار طراحی شده است. بات ها را می توان برای کنترل رایانه‌ای قربانی توسط یک مهاجم از راه دور یا نفوذگر بدخواه به کار برد. ماهیت برخی بات ها به گونه‌ای است که کنترل صدهزار رایانه شخصی را به اندازه کنترل یک رایانه آسان می‌کند. بات ها می توانند برای ارسال هرزنامه، دریافت و ذخیره فایل‌های غیرقانونی، یا شرکت دادن رایانه‌ها در حمله به سایر رایانه‌ها استفاده شوند. یک بات می‌تواند رایانه قربانی را جستجو کرده و اطلاعات محرمانه را به یک پایگاه دور بر روی اینترنت بفرستد. رایانه‌هایی که توسط بات ها به طور ناخودآگاه در خدمت نفوذگران بدخواه قرار می‌گیرند، زامبی (zombie) نامیده می شوند.
botnet	شبکهٔ بات	شبکه‌ای از رایانه‌های زامبی که تحت کنترل و فرمان یک مهاجم برای حمله به مقاصد خاص مورد استفاده قرار می-گیرند.
bottleneck	گلوگاه	نقطه یا گره‌ای در شبکه که حجم تبادل داده در آنجا زیاد باشد.
bouncer (BNC)	نگهبان	نگهبان که اغلب به صورت خلاصه BNC نمایش داده می‌شود برای هماهنگ کردن ترافیک و اتصالات در شبکه های رایانه‌ای به کار می رود. با استفاده از آن می توان منبع اصلی اتصال کاربر را پنهان کرده و از این طریق، حریم خصوصی را ضمن امکان مسیریابی ترافیک از یک مکان خاص فراهم نمود.
bound	کران	
boundary protection	حفاظت مرزی	نظارت و کنترل ارتباطات بین مرزهای خارجی مابین یک سامانه اطلاعاتی داخلی سازمان، و یک سامانه اطلاعاتی خارجی، و یا بین مرزهای حساس بین سامانه‌های اطلاعاتی داخلی، جهت جلوگیری و کشف ارتباطات مخرب و غیرمجاز، و با استفاده از واسط‌های کنترلی مانند حفاظ، مسیریاب، دروازه، تونل رمز شده و غیره.
BPP complexity class	ردهٔ پیچیدگی BPP	اختصار برگرفته از عبارات Bounded-errot، Probablistic و Polynomial-time . در نظریه پیچیدگی به دسته‌ای از مسائل تصمیم اطلاق می-شود که با احتمال خاص در یک زمان چندجمله‌ای قابل حل

		هستند.
branch number	عدد انشعاب	حداقل تعداد عناصر تغییر یافته در یک زمان در ورودی وخروجی لایه مخلوط ساز(mixing layer) به ازای تمامی تغییرات ممکن ورودی.
breach	رخنه	
break	شکستن	حمله‌ای که با تلاشی کمتر از آنچه در طراحی الگوریتم رمز برای امنیت آن ادعا شده منجر به یافتن کلید شود. (یعنی کمتر از جستجوی فراگیر فضای کلید).
breakable	قابل شکست	هرگاه دستیابی به کلید از روی متن رمز شده و متن اصلی آن با پیچیدگی کمتر از جستجوی فراگیر فضای کلید امکان پذیر باشد.
bridge	پل	ابزاری است که در لایه پیوند داده‌ها عمل کرده و شبکه‌های محلی (LAN) را به هم متصل می‌کند.
bridge firewall	حفاظ پل	
broadcast	پخش	پخش وانتشار امواج برای کاربری همگانی مانند رادیو و تلویزیون.
broadcast encryption	رمزگذاری پخش	روش موثری برای پخش همگانی اطلاعات به گروهی دائماً در حال تغییر، به صورتی که فقط افراد دارای مجوز دریافت اطلاعات، امکان رمزگشایی آن را داشته باشند.
browser	مرورگر	
brute force attack	حملهٔ جستجوی فراگیر	حمله‌ای که در آن تمام حالات ممکن تا رسیدن به جواب بررسی می شود.
buffer	بافر، حافظهٔ میانی	
buffer overflow	سرریز بافر	وقتی در یک برنامه یا فرآیند، بیش از حد ظرفیت حافظه میانی در آن ذخیره شود، حافظه سرریز می کند که به آن سرریز حافظه میانی گفته می شود.
buffer overflow attack	حملهٔ سرریز بافر	حمله‌ای که با بار گذاری بیش از حد ظرفیت یک حافظه میانی، باعث سر ریز شدن آن شده و موجب اختلال در کار رایانه می شود.
bug	اشکال	
built-in	توکار	
burst error	خطای قطاری	خطای پیاپی نامنظم که در یک دنباله تحت تاثیر اغتشاش ناگهانی به وجود می آید.
business continuity plan (BCP)	طرح تداوم کسب و کار	مستنداتی متشکل از مجموعه‌ای معین از دستورات و رویه‌ها

		که نحوه تداوم عملکرد سازمان را در حین و پس از یک بحران مهم توصیف می نماید.
business impact analysis (BIA)	تحلیل تأثیر کسب و کار	تحلیلی از نیازمندی‌ها، فرایندها، و وابستگی بین مؤلفه‌های یک سامانه فناوری اطلاعات، که جهت توصیف وابستگی‌ها و اولویت‌های سامانه در هنگام رخداد یک بحران مهم، مورد استفاده قرار می‌گیرد.
business recovery-rsumption plan (BRP)	طرح بازیابی کسب و کار	مستنداتی متشکل از مجموعه‌ای معین از دستورالعمل‌ها و رویه‌ها که نحوه ترمیم، پس از رخداد یک بحران مهم را توصیف می کند.
bypass	کنارگذر	
C		
CA→Certification Authority		
cache consistency	سازگاری حافظهٔ نهان	
caching	نهان سازی	
Caesar cipher	رمز سزار	یک نوع رمز جانشینی ساده، که در آن هر حرف با حرفی که به تعداد مشخص و ثابتی در الفبا جلوتر از آن است، جایگزین می‌شود. برای مثال با فرض عدد انتقال سه، حرف "الف" با حرف "ت" وحرف "ب" با حرف "ث" جایگزین می شود.
Camellia cipher	رمز کاملیا	یک نوع سیستم رمزنگاری قالبی.
captcha		کلمه اختصاری برای Capture Character، ابزاری برای جلوگیری از کاربرد روش‌های خودکار در ورود داده به فرم‌های تحت وب.
capture	اخذ	۱. گرفتن نمونه زیست سنجشی از یک کاربر. ۲. فرآیند دریافت و ذخیره‌سازی اطلاعات برای استفاده درآینده، مانند دریافت تصویر و ضبط صدا.
captured	دزدیده شده	
card issuer	صادر کننده کارت	واحد یا مؤسسه‌ای که کارت (هوشمند) را برای مقاصد خاص صادر می‌کند.
cardholder	صاحب کارت	فردی که صاحب یک کارت PIV(Personal Identity Verification) است.
cascade cipher	رمز متوالی	یک سامانه رمزنگاری که از کنارهم چیدن چند سیستم رمز به صورت متوالی تشکیل می‌شود.
CBC → Cipher Block		

Chaining mode		
centralized directory service	خدمت راهنمایی متمرکز	
CERT → Computer Emergency Response Team		
certificate	گواهی‌نامه	یک نمایش دیجیتالی از اطلاعات که حداقل شامل نام مرجع صدور گواهی، نام صاحب گواهی‌نامه، کلید عمومی او، دوره اعتبار و تاریخ انقضاء گواهی است و توسط مرجع صدور گواهی امضای دیجیتال شده است.
certificate of primality (or primality certificate)	گواهی اول بودن	در ریاضیات و علوم کامپیوتر به مجموعه‌ای موجز از اطلاعات اطلاق می شود که به یک عدد اول ملحق می شود و برای تسریع در اثبات اول بودن آن عدد (بدون نیاز به اجرای آزمون‌های پیچیده) به کار می رود.
certificate revocation list (CRL)	فهرست گواهی‌های باطل‌شده (فسخ شده)	فهرستی از گواهی‌نامه های (کلید عمومی) فسخ شده که توسط مرجع صدور گواهی تولید، به روز، امضا و منتشر می شود.
certificate-related information	اطلاعات مرتبط با گواهی‌نامه	اطلاعاتی همچون آدرس پستی فرد که در گواهی قرار نمی-گیرد. این اطلاعات ممکن است در مدیریت گواهی توسط مرجع صدور گواهی (CA) مورد استفاده قرار گیرد.
certification	گواهی	روند صدور گواهی‌نامه برای تایید شیء، شخص و یا یک نهاد مشخص.
certification and accreditation (C&A)	صدور گواهی و اعطای اعتبار	فرآیندی رسمی برای اخذ تاییدیه، جهت حصول اطمینان از پیاده سازی و اجرایی نمودن صحیح ملزومات، کنترل‌ها و روال‌های امنیتی که به منظور به حداقل رساندن هرگونه تهدید در SAAA (Security Authority Authorization Agreement) مدنظر قرار گرفته است. اخذ این تاییدیه از سال ۲۰۰۲ در آمریکا برای محصولات مورد استفاده در نهادهای دولتی اجباری است.
certification authority (CA)	مرجع صدور گواهی	نهادی رسمی و مورد اعتماد که وظیفه صدور، مدیریت، انتشار و فسخ گواهی‌نامه‌های کلید همگانی را بر عهده دارد.
certification policy	خط‌مشی گواهی	
certification sign request (CRS)	درخواست امضای گواهی	
CFB →Ciphertext Feedback Operating mode		

chaffing and winnowing	کاه دادن و باد دادن	روشی جهت محرمانه کردن پیام از دست دشمن بدون رمزنگاری، در این روش پیام به بسته‌های کوچک تر شکسته شده و به هر بسته کد احراز اصالت اضافه می‌شود. سپس در میان بسته‌های اصلی تعدادی بسته‌های اضافی (با کد احراز اصالت تصادفی) به نام کاه اضافه می‌شود. طرف مقابل که از کلید احراز اصالت آگاهی دارد، می‌تواند بسته‌های اصلی(گندم) را از بسته‌های ساختگی(کاه) تشخیص دهد و با جدا کردن کاه از پیام، آن را بازسازی کند. به این عمل باد دادن گفته می شود. ولی دشمن که از کلید کد احراز اصالت بی‌خبر است، نمی‌تواند بسته های اضافی را از بسته های اصلی جدا کرده و پیام را بازسازی کند.
chain	زنجیره	اعمالی که به صورت متوالی اجرا می‌شوند و ورودی هر قسمت وابسته به خروجی مرحله قبل است، مانند آنچه در سبک اجرایی CBC صورت می گیرد.
chain of custody	زنجیرهٔ حفاظت	زنجیره‌ای از فرآیندها شامل مستندسازی، ضبط، نگهداری، کنترل، انتقال، تحلیل، و صورت‌بندی شواهد فیزیکی و الکترونیکی(وقوع جرم).
chaining attack	حملهٔ زنجیره ای	
challenge message	پیام چالش	
challenge-response authentication	احراز اصالت مبتنی بر چالش و پاسخ	یک نوع پروتکل احراز اصالت که در آن طی یک فرآیند پرسش و پاسخ هویت یک شناسه اثبات می‌شود.
change point test	آزمون نقطه عطف	آزمونی آماری برای بررسی رفتار تصادفی یک دنباله. نقطه عطف یک دنباله مکانی است که در آن مشحصات آماری دنباله تغییر می کند. هدف از انجام این آزمون یافتن نقطه عطف دنباله (در صورت وجود) و تعیین میزان اهمیت آن نقطه است.
chaotic function	تابع آشوبی	
character	نویسه	
characteristic	مشخصه	
characteristic frequency	بسامد مشخصه (حروف)	فراوانی حروف در متن
characteristic polynomial	چند جمله ای مشخصه	
check list	فهرست بررسی	
checksum	جمع آزما، سرجمع	
chinese remainder	قضیه باقیمانده چینی	

theorem (CRT)		
chinese wall security policy	خط‌مشی امنیتی دیوار چین	یکی از خط مشی‌های کنترل دسترسی در حوزه تجارت الکترونیک.
chosen ciphertext attack	حملهٔ متن رمز منتخب	حمله‌ای که در آن تحلیل‌گر می‌تواند هر متن رمزی را که بخواهد قبل از انجام حمله انتخاب کند تا برایش رمزگشایی شود.
chosen IV attack	حمله براساس بردار اولیه منتخب	
chosen plaintext attack	حملهٔ متن اصلی منتخب	در این حمله دشمن می تواند هر متنی را که بخواهد، قبل از شروع حمله، انتخاب کند تا برایش رمز شود. این امر مثل آن است که ماشین رمز کننده قبل از انجام حمله در اختیار دشمن باشد و فقط از کلید آن آگاهی نداشته باشد. به این نوع حمله، «حمله نوع سوم» نیز گفته می‌شود. اگر دشمن بر مبنای متون رمزشده متن‌های انتخابی‌اش، این امکان را داشته باشد که متن‌های دیگری را برای رمزشدن انتخاب کند، حمله از نوع متن اصلی منتخب وفقی نامیده می‌شود.
cipher	رمز	سامانه‌ای وابسته به کلید جهت تبدیل یک متن به متنی سرّی که توسط غیر، قابل درک نباشد.
cipher block chaining mode(CBC)	سَبک زنجیره‌ای قالب‌های رمز	یک سبک اجرایی برای استفاده از رمزهای قالبی، در این روش اولین قالب متن رمز، از رمز شدن حاصل جمع اولین قالب متن اصلی با مقدار اولیه(IV) تولید می شود. قالبهای بعدی از رمز شدن حاصل جمع قالب متن اصلی و قالب متن رمز قبلی بدست می آیند.
cipher feedback mode(CFB)	سَبک پسخورد رمز	یک سبک اجرایی برای استفاده از رمزهای قالبی، در این روش اولین قالب متن رمز از جمع مقدار اولیه رمز شده با متن اصلی بدست می‌آید، قالب‌های بعدی از جمع رمز شده قالب قبلی متن رمز و قالب جدید متن اصلی حاصل می‌شود. این سبک بیشتر در ایجاد دنباله شبه تصادفی و طراحی رمزهای دنباله‌ای کاربرد دارد.
ciphertext	متن رمز شده، متن رمز	خروجی تابع رمزنگاری، در مقابل plaintext
ciphertext only attack	حمله فقط براساس متن رمز	در این حمله دشمن باید فقط با داشتن متن رمز شده کلید را بدست بیاورد. معمولا در این حمله از خواص آماری رمز استفاده می شود. به این نوع حمله، «حمله نوع اول» نیز گویند.

ciphony	رمزآوا	رمز کردن مکالمات تلفنی
circuit level firewall	حفاظ سطح مسیر	نوعی حفاظ که در لایهٔ نشست از مدل OSI (و یا بین لایه‌های کاربرد و انتقال در مدل TCP) کار می‌کند. حفاظ بر دستداد بین بسته‌ها نظارت می‌کند تا تعیین کند که آیا نشست مورد درخواست مجاز است یا نه. برای این منظور هر اتصال بین مبدأ و مقصد به دو اتصال تبدیل می‌شود: اتصال مبدأ–حفاظ، و اتصال حفاظ–مقصد.
circuit level gateway	دروازه سطح مسیر	
claimant	مدعی	موجودیتی که اصالتش باید توسط یک پروتکل احراز شود.
class	رده	
classic ciphers	رمزهای سنتی	رمزهایی که پیشینه تاریخی دارند و قبلاً مورد استفاده قرار می گرفته‌اند، ولی در حال حاضر به دلیل پیشرفت فناوری و تکنیک‌های تحلیل رمز امنیت آن‌ها از بین رفته و استفاده از آن‌ها منسوخ شده است. این نوع رمزها به دو دسته رمزهای جانشینی و رمزهای جابجایی تقسیم می شوند.
classification	رده بندی	
classified data	داده های طبقه بندی شده	
classifier	رده بند	
claw-free= claw-resistant	بی چنگ	به زوج توابع f وg بی چنگ گفته می شود، هرگاه پیدا کردن ورودیهایی مثل x و y که به ازای آنها دو تابع دارای خروجی یکسان ، یعنی f(x)=g(y) باشند ، مشکل باشد.
clear channel assessment attack	حملهٔ ارزیابی کانال آشکار	یک نوع حمله منع خدمت در شبکه‌های بی‌سیم Wi-Fi که در لایه فیزیکی شبکه اعمال می‌شود.
cleartext = plaintext	متن اصلی	پیام رمز نشده
clickjacking	سرقت کلیک	مخفی‌سازی لینک‌ها و دکمه‌ها به نحوی که کاربر ناخواسته روی آن‌ها کلیک کند.
client	کارخواه، مشتری	
client/server model	مدل کارخواه/کارگزار	
Clipper chip	تراشهٔ کلیپر	یک تراشه برای پیاده سازی الگوریتم Skip-Jack که امکان امان سپاری کلیدرا فراهم می ساخت. این تراشه در سال ۱۹۹۳ به عنوان یک ابزار رمزنگاری ارائه و در سال ۱۹۹۶ به دلیل عدم اقبال از صحنه خارج شد.
clock-controlled generator	مولد با فرمان ساعت	
clogging attak	حملهٔ انسداد	یک نوع حمله منع خدمت علیه سامانه‌های رمز کلید

		همگانی. در این نوع حمله، مهاجم نسخه‌هایی از کلیدهای همگانی را به نشانی کاربر هدف می‌فرستد تا منابع این کاربر برای بررسی کلیدهای دریافتی به نحوی صرف شود که امکان ارتباط از سوی کاربران واقعی سلب گردد.
closed/open world policy	خط مشی دنیای بسته/باز	خط مشی‌ای که در محیط‌های کنترل دسترسی برای حالتی که دسترسی با هیچ قانونی تطابق نمی‌کند اتخاذ می‌شود.
closest vector problem(CVP)	مسئلهٔ نزدیک ترین بردار	یک مسئله محاسباتی در مشبکه‌ها است که در آن یافتن یک عضو از مشبکه با کمترین فاصله ممکن از یک بردار داده شده (نقطه هدف) دنبال می شود. این مسئله از مسائل رده NP است و تعدادی الگوریتم رمزنگاری بر مبنای آن طراحی شده است.
closure attack	حملهٔ بستاری	
clueless	بی خبر	
cluster analysis	تحلیل خوشه‌ای	
code	کد	هر آنچه به عنوان نشانه و یا نماینده چیزی می‌آید. این نشانه می تواند عدد، شکل ، رنگ و یا هر چیز دیگری باشد. ولی معمولاً از اعداد برای کدگذاری استفاده می شود.
code breaker	رمز شکن	
code maker	رمزساز	
codebook	کتاب کد	کتابی که شامل لیستی از کلمات و نشانه‌های (کدهای) متناظر با آنهاست.
codebook attack	حملهٔ کتاب کُد	حمله‌ای که در آن دشمن سعی دارد با جمع‌آوری و تهیه کتاب کد، همه تبدیل‌های بین متن‌های اصلی و رمزشده آن-ها (توسط یک کلید ثابت) را ثبت کند. برای جلوگیری از اعمال این حمله علیه رمزهای قالبی، طول قالب باید به اندازه کافی بزرگ باشد، و یا رمز در سبک های اجرایی نظیر سبک زنجیره‌ای (CBC) استفاده شود.
coding	کدگذاری	
coercion resistance	عدم اجبار	
cold site = shell site	پایگاه خالی، پایگاه پوسته	یک تشکیلات پشتیبان که تمامی امکانات الکتریکی و فیزیکی یک سایت کامپیوتری را دارا بوده، ولی هیچ کامپیوتری در آن وجود ندارد. این تشکیلات در هنگام تعویض مکان سایت اصلی مورد استفاده قرار می‌گیرد.
collision	برخورد	معمولا در مورد توابع چکیده‌ساز که فضای مقادیر خروجی

		محدود و فضای مقادیر ورودی بسیار وسیع (و یا حتی نا محدود) است به‌کار برده می شود و به دو ورودی متمایز که دارای مقدار یکسان در خروجی تابع باشند، اطلاق می‌شود.
collision free	بدون برخورد	یکی از ویژگی‌های یک تابع چکیده‌ساز است که به ازای یک ورودی ثابت، پیدا کردن ورودی دیگری با همان مقدار خروجی، مشکل باشد.
collision free hash function	تابع چکیده ساز بدون برخورد	
collision resistance	مقاومت در برابر برخورد	یکی از ویژگی‌های توابع چکیده‌ساز که پیدا کردن یک زوج ورودی دلخواه با خروجی یکسان، از لحاظ محاسباتی غیر ممکن باشد.
combining function	تابع ترکیب کننده	
commitment protocol	پروتکل تعهد	یک پروتکل دو مرحله‌ای بین طرفین ارتباط، در مرحله اوّل (تعهد) فرستنده به یک مقدار که نمی‌تواند بعداً آن را تغییر دهد و آن را به صورت پوشیده برای گیرنده ارسال می‌کند متعهد می‌شود.در مرحله دوّم (واپوشی) فرستنده اطلاعات اضافی دیگری برای گیرنده ارسال می‌کند که واپوشی و اطلاع از مقدار تعهد شده را برای او میسر می کند.
common vulnerabilities and exposures (CVE)	آسیب پذیری ها و رخنه‌پذیری‌های متداول	فهرستی از آسیب پذیری‌های عمومی شناخته شده در سامانه-های فناوری اطلاعات
communications security(COMSEC)	امنیت مخابرات	واژه‌ای اختصاری جهت مقاصد نظامی که زمینه های مختلفی از امنیت، نظیر رمزنگاری، امنیت ارسال داده (ملاحظات الکترومغناطیس)، امنیت فیزیکی (قابلیت دسترسی) و مسائلی نظیر تحلیل ترافیک، طیف گسترده، کاهش میزان آشکار سازی و ... را شامل می‌شود.
compatibility	سازگاری	
complementation property	ویژگی مکملیت	یک تابع رمزکننده با ورودی x و کلید k دارای ویژگی مکمّلیت است، هرگاه: $\forall x, k \quad f_{\bar{k}}(\bar{x}) = f_k(x)$
completeness property	ویژگی تمامیت	وقتی هر بیت خروجی یک تابع تحت تاثیر تمامی بیت‌های ورودی باشد، گوییم تابع دارای ویژگی تمامیت است.
complexity theory	نظریهٔ پیچیدگی	
component	مولفه	
compression function	تابع فشرده ساز	معمولاً یکی از اجزای یک تابع چکیده ساز، تابعی است که یک ورودی با طول ثابت را به یک خروجی با طول ثابت، ولی کوچکتر تبدیل می کند.

compromise	به مخاطره افتادن، تسخیرشدن، لو رفتن	افشای اطلاعات به افراد غیر مجاز، و یا نقض یک خط مشی امنیتی در سامانه‌ای که در آن افشا و یا تغییر عمدی یا سهوی اطلاعات رخ داده است.
compromising emanations	برون تابی‌های مخاطره آمیز	انتشار شکل‌هایی از انرژی از یک تجهیزات اطلاعاتی مثل رایانه که می‌تواند به طور ناخواسته موجب نشت اطلاعات شود، مثل تشعشعات رادیویی، سیگنالهای نوری و اعوجاجات توان مصرفی
computational complexity	پیچیدگی محاسبات	مرتبه زمانی اجرای یک الگوریتم، میزان تلاش محاسباتی است که باید برای حل یک مسئله (معمولا اجرای یک الگوریتم) صرف شود. در تحلیل رمز، این مقدار در اندازه-گیری میزان کار (زمان) لازم برای انجام یک تحلیل مهم است. در تحلیل رمزهای قالبی، پیچیدگی محاسباتی حمله معمولاً بر حسب میزان محاسبات لازم برای رمزنگاری یک قالب داده توسط همان سیستم رمز بیان می‌شود.
computational complexity theory	نظریه پیچیدگی محاسبات	شاخه‌ای از علوم کامپیوتر است که در آن میزان منابع لازم برای اجرای یک الگوریتم مانند زمان، حافظه،... مورد بررسی قرار می‌گیرند.
computationally secure	امن محاسباتی	گوییم یک سامانه رمز دارای امنیت محاسباتی است، هرگاه شکستن آن با توجه به محدویت های موجود در امکانات محاسباتی و زمان تحلیل عملاً امکان پذیر نباشد. (در حالی که ممکن است از لحاظ نظری امن نباشد.)
computer crime	جرم رایانه ای	
computer emergency response team (CERT)	گروه واکنش اضطراری رایانه (آپا)	یک گروه کاری که با داشتن تخصص در یک حوزه مشخص به نیازهای فوری کاربران در زمینه حوادث رایانه‌ای پاسخ می‌گویند. سرنام "آپا" از ترجمه مفهومی "آگاهی رسانی، پشتیبانی و امداد در حوادث رایانه‌ای" گرفته شده است.
computer forensics	بررسی جرایم رایانه‌ای	فرایند جمع‌آوری، و تحلیل داده‌های کامپیوتری به منظور بازرسی رخدادهای ناقض امنیت در سامانه‌های فناوری اطلاعات
computer fraud	تقلب رایانه‌ای	
computer security	امنیت رایانه‌ای	
COMSEC → Communications Security		

concatenate	الحاق	
concealment	پنهان‌سازی	
concurrent	هم‌روند	
concurrent connection	اتصال هم‌روند	
conditional security	امنیت مشروط	
conference keying protocol	پروتکل تولید کلید جلسه کنفرانس	پروتکلی به منظور برقراری یک ارتباط امن بین اعضای یک گروه با حداقل سه عضو از طریق تولید و توزیع یک کلید مشترک رمزنگاری بین آن ها.
confidentiality	محرمانگی	
configuration	پیکربندی	
configuration control	کنترل پیکربندی	فرآیند کنترل تغییرات سخت افزار، سفت افزار و نرم افزار و مستندات، به منظور کسب اطمینان از این که سامانه اطلاعات، در برابر تغییرات نامناسب، قبل، در خلال و پس از پیاده سازی سامانه حفاظت شده است.
confirmation	تایید	
confounder	آشفته ساز	
confusion	آشفته سازی	یکی از دو قاعده‌ای که شانون برای مقاوم کردن رمزها پیشنهاد کرد. این قاعده بیان می کند که وابستگی خواص آماری متن رمز به خواص آماری متن اصلی باید چنان پیچیده باشد که تحلیلگر نتواند آن را کشف کند. (بدین منظور از تبدیلات جانشینی برای پیچیده کردن رابطه بین کلید و متن رمز شده استفاده می‌شود.) روش دیگر، ایجاد پراکنش(diffusion) است.
connection handling stage	مرحلهٔ پردازش اتصال	
connection maintenance	نگهداری اتصال	
connection oriented	اتصال‌گرا	
connection setup / connection establishment	ایجاد اتصال	
connection teardown	خاتمهٔ اتصال	
connectionless	بدون اتصال	
consistency	هم‌سازی، همخوانی	
console	پیشانه، پیشخوان	
constraint	قید	
content filter	صافی محتوا	

content format	قالب محتوا	
contingency plan	طرح رخداد پذیر	خط‌مشی مدیریتی و رویه‌های طراحی شده به منظور تداوم یا بازیابی عملیات، در صورت وقوع خرابی در سامانه یا رخداد بلایای طبیعی.
contract	قرارداد	
control connection	اتصال کنترلی	
conventional cryptosystem	سامانهٔ رمزنگاری متعارف	همان سامانه رمزنگاری متقارن است که کلید دو طرف یکسان است.مثل AES
cookie	کلوچک	یک فایل که به درخواست یک پایگاه وبِ راه دور روی دیسک سخت رایانه نوشته و یا از روی آن خوانده می شود. مثلاً اگر به پایگاه وب، نام کاربری خود را بدهید، می‌تواند درخواست کند که آن اطلاعات روی دیسک شما نوشته شود. زمانی که دوباره به آن پایگاه وب مراجعه می کنید، آن پایگاه کلوچک مربوطه را از روی دیسک رایانه شما می خواند و متوجه می شود که نام کاربری شما چه بوده است. کلوچک‌ها برای تهیه سابقه‌ای از عادت‌های گردش در وب به کار گرفته می شوند و در بعضی موارد ممکن است حریم خصوصی کاربران را نقض کنند.
coprime	متباین، نسبت به هم اول	گوییم اعداد صحیح a و b متباین(نسبت به هم اول) هستند، هرگاه بزرگترین مقسوم علیه مشترک آنها برابر با یک باشد.
copy protection	ممانعت از نسخه برداری	
copyleft	حق واگذاری	یادداشت حقوقی که برمبنای آن امکان بهبود، استفاده مجدد و باز تولید یک اثر برای تمام کاربران به رسمیت شناخته می-شود.
copyright	حق نسخه‌برداری	
correcting block attack	حملهٔتصحیح قالب	حمله‌ای علیه توابع چکیده ساز، این حمله جهت یافتن برخورد و یا پیش تصویر به کار برده می‌شود.
correlation	همبستگی	
correlation attack	حملهٔ همبستگی	یکی از مشهورترین حملات قابل اعمال روی رمزهای دنباله-ای و به خصوص رمزهای مبتنی بر LFSR است. در این حمله تلاش می شود از همبستگی موجود بین دنباله کلید اجرایی و ترکیبات خطی مختلف بیت های کلید، برای یافتن کلید استفاده شود. این حمله اولین بار در سال ۱۹۸۵ توسط Siegenthaler معرفی شد.

correlation immunity	ایمنی از همبستگی، مصونیت از همبستگی	در حالت کلی کمینه کردن اطلاعات متقابل بین خروجی یک تابع بولی و بردار ورودی آن بی معناست، زیرا با دانستن ورودی یک تابع بولی، خروجی آن به صورت یکتا مشخص می شود. اما می توان اطلاعات متقابل بین خروجی و زیر بردارهای ورودی را کمینه کرد. گوییم تابع بولی n متغیره f دارای مصونیت از همبستگی از مرتبه k است، هرگاه اطلاعات متقابل بین خروجی و همه زیر بردارهای k تایی از متغیرهای ورودی صفر باشد.
correlation power analysis attack (CPA)	حملهٔ تحلیل همبستگی توان	رجوع کنید به power analysis attack
counter mode= integer counter mode, segmented integer counter mode	سَبک شمارنده	یک نوع سبک اجرایی برای استفاده از رمزهای قالبی. در این روش متن رمز از جمع متن اصلی با رمز شده مقدار شمارنده حاصل می شود.
counterexample	مثال نقض	
countermeasure	پارسنگ، اقدام متقابل	معادل واژه کنترل های امنیتی و قواعد حفاظتی. اَعمال، رویه‌ها، تکنیک ها، و یا هر اقدام دیگری که جهت کاهش آسیب پذیری یک سامانه اطلاعاتی اتخاذ می گردد.
cover object	شیئ پوششی	منظور از شیئ پوششی، متن یا تصویری است که در آن پیامی تعبیه می شود.
covert channel	کانال پنهان	کانال پنهان روشی برای ارسال مخفی داده‌های غیر مجاز با پنهان کردن آن‌ها در قسمتی از بسته‌هاست که به طور معمول برای ارسال داده استفاده نمی‌شوند . به این ترتیب اطلاعات بدون دخالت حفاظ و یا سامانهٔ تشخیص نفوذ نشت پیدا می-کند.
CPA→Correlation Power Analysis Attack		
cracked	قفل شکسته	
cracker	قفل‌شکن	فردی که معمولا با نیت سوء جهت قفل شکنی یک نرم افزار و یا دستیابی غیر مجاز به گذرواژه‌های یک شبکه تلاش می کند.
cracking	قفل شکنی	ایجاد تغییرات غیر قانونی در یک نرم افزار تجاری و یا دور زدن رویه‌های احراز اصالت و یا رمزگشایی غیر مجاز یک ارتباط.
CRC→Cyclic Redundancy Check		
credentials	اعتبارنامه	مدرکی دال بر حق، اعتبار، یا مسئول بودن کسی

credentials service provider	تأمین کننده خدمات اعتبارنامه ها	یک موجودیت مورد اعتماد که نشانه‌های متقاضی را بررسی و ثبت می‌کند و اعتبارنامه الکترونیکی برای وی صادر می-کند.
credit card	کارت اعتباری	
critical security parameter	پارامتر امنیتی بحرانی	اطلاعات مرتبط با امنیت مانند کلیدهای رمزنگاری خصوصی و داده‌های احراز اصالت نظیر گذرواژه‌ها و شماره‌های شناسایی شخصی (PIN) که افشا یا تغییر آنها می تواند امنیت یک واحد رمزنگاری را به خطر اندازد.
criticality level	سطح بحران	به پیامدهای عملکرد نادرست یک سامانه اشاره دارد. هر قدر تأثیر عملکرد صحیح یا نادرست یک سامانه جدی تر باشد، سطح حساسیت بالاتر است.
CRL→Certificate Revocation List		
cross certificate pair	زوج هم‌گواه	
cross certification	گواهی متقابل	
cross correlation	همبستگی متقابل	
cross site scripting(XSS)	نبشته سایت قلابی	این آسیب‌پذیری به مهاجم اجازه می‌دهد نبشته مورد نظرش را در مرورگر قربانی اجرا کند. برای مثال یک نامه الکترونیکی به صندوق پستی قربانی ارسال می‌شود که عنوانی با مضمون برنده شدن وی در یک قرعه‌کشی دارد و کاربر را به گشودن آن ترغیب می‌کند. اما با باز شدن نامه الکترونیکی، نبشته فرستاده شده توسط مهاجم اجرا شده و سامانه وی مورد حمله قرار می‌گیرد.
CRS→Certification Sign Request		
CRT→Chinese Remainder Theorem		
cryptanalysis	تحلیل رمز، رمزشکنی	دانشِ روش‌ها و راهکارهای مختلفی که تحلیل‌گر برای تحلیل و شکستن رمز به کار می برد. (تحلیل و شکستن رمز= پیدا کردن کلید یا دستیابی به اصل پیام با تلاشی کمتر از جستجوی فراگیر فضای کلید)
cryptanalyst	تحلیل‌گر رمز، رمزشکن	کسی که اجازه فهمیدن کلید و یا متن اصلی را ندارد، ولی با روش‌هایی سعی در یافتن کلید و یا متن اصلی دارد.
crypto-anarchism	اخلال رمزنگاشتی	
cryptogram	رمزنگاشت	
cryptographer	رمزنگار	

cryptographic	رمزنگاشتی	
cryptographic strength	استحکام رمزنگاشتی	
cryptographic token	نشان رمزنگاشتی	
cryptography	رمزنگاری	علم و هنر سرّی کردن داده‌ها، رمزنگاری نامیده می‌شود. کاربردهای رمزنگاری در حال حاضر تنها به سری کردن داده‌ها محدود نمی‌شود، از سایر کاربردهای طرح‌های رمزنگاری می‌توان به احراز اصالت، انکارناپذیری و حفظ یکپارچگی پیام اشاره کرد.
cryptological	رمزشناختی	
cryptologist	رمزشناس	
cryptology	رمزشناسی	مجموعه علوم مشتمل بر رمزنگاری (cryptography) و تحلیل رمز (cryptanalysis).
cryptoperiod	رمز دوره	بازه زمانی که کلید رمز معتبر است.
cryptosystem	سامانهٔ رمز	
CTR→Counter mode		
cut and paste attack	حملهٔ بریدن و چسباندن	
cut-and-choose protocol	پروتکل برش و انتخاب	
CVE→Common Vulnerabilities and Exposures		
cyber liability	مسئولیت فضای تبادل اطلاعات	
cyber terrorist	تروریست(خرابکار) فضای تبادل اطلاعات	
cyber→ cyberspace		
cybercrime	جرم فضای تبادل اطلاعات	فعالیت‌های مجرمانه‌ای که در فضای تبادل اطلاعات صورت می گیرد.
cyberspace	فضای تبادل اطلاعات	آنچه مربوط به فناوری اطلاعات، اینترنت و فضای مجازی است.
cyclic	چرخه‌ای، دوری	
cyclic code	کد دوری	
cyclic group	گروه دوری	
D		
data	داده، داده ها	
data compaction	چکیده سازی داده‌ها، فشرده	

	سازی داده‌ها	
data complexity	پیچیدگی داده ها	
data compression	فشرده سازی داده‌ها	
data conversion	تبدیل داده ها	
data custodian	داده بان	
data deciphering	رمزگشایی داده‌ها	
data decryption	رمزگشایی داده‌ها	
data encryption	رمزگذاری داده‌ها	
data integrity	تمامیت داده، یکپارچگی داده	
data link layer	لایه پیوند داده‌ها	
data message integrity	یکپارچگی داده پیام	
data mining	داده کاوی	
data perturbation	آشفتگی داده	
data port	درگاه داده	
data protection	حفاظت داده ها	
data remanence	پسماند داده ها	
data restoration	ترمیم داده	عمل تولید مجدد داده‌ای که از دست رفته یا آلوده شده است.
data seal	مهر و موم داده ها	
data security	امنیت داده	
data stream	جریان داده	
database	دادگان، پایگاه داده ها	
data-driven attack	حملهٔ داده–مبنا	
datagram	بستک	
DC→Differential Cryptanalysis		
dealer	تسهیم کننده، توزیع کننده	
debit card	کارت پیش پرداخت	
debug	اشکال زدایی	
decentralization	تمرکز زدایی	
decimated subsequence	زیردنبالهٔ ورچین شده	زیردنباله‌ای که با انتخاب یک نمونه از هر چند نمونه از دنباله اصلی حاصل شود.
decimation	چند به یک کردن، برچیدن، ورچیدن	

decipher	رمزگشایی کردن	عمل برگرداندن متن رمز شده به متن اصلی توسط کلید. در مقابل encipher
decision tree	درخت تصمیم گیری	
decode	کدگشایی کردن	
decoder	کدگشا	
decoding attack	حملهٔ کدگشایی	یکی از انواع حملات به سامانه‌های رمزنگاری که مبتنی بر نظریه کدگذاری اعمال می‌شود. در این حمله دشمن از طریق متن رمز و کدبرداری از آن سعی در بدست آوردن پیام دارد.
decrypt	رمزگشایی کردن	
decryption	رمزگشایی	در مقابل encryption
DECT (Digital Enhanced Cordless Telecommunications)		استاندارد رادیویی برای ارتباط بی سیم در فواصل کوتاه که برای انتقال داده، صدا و کاربردهای شبکه‌ای تا فاصله ۵۰۰ متر به کار می رود.
deduction	استنتاج، قیاس	
defined plaintext attack → chosen plaintext attack		
demilitarized zone (DMZ)	منطقهٔ بی‌طرف، منطقهٔ حائل	ناحیه‌ای از شبکه که خدمات عمومی به بیرون (نظیر کارگزار وب) را فراهم می‌کند. این ناحیه بین شبکهٔ داخلی و شبکهٔ بیرونی (اغلب اینترنت) قرار می‌گیرد.
deniable authentication	احراز اصالت حاشاپذیر	یک نوع احراز اصالت بین اعضای یک گروه که افراد می‌توانند بین خود، عمل احراز اصالت را انجام دهند، ولی به نفر سومی خارج این مجموعه نمی‌توانند هویت خود را ثابت کنند.
deniable encryption	رمزگذاری حاشاپذیر	رمزگذاری حاشاپذیر امکان انکار را در صورت لزوم برای شخص رمزگذار فراهم می‌آورد. بدین معنا که وی قادر است برای متن رمزشده مفروض، به‌نحوی که ناظر یا طرف سوم را متقاعد سازد، به جای متن اصلی واقعی متن اصلی دیگری ارائه دهد.
denial of authentication attack	حملهٔ منع احراز اصالت	
denial of quality of service (DoQoS)	حملهٔ کاهش کیفیت خدمت	
denial of service attack (DoS)	حملهٔ منع خدمت	در این حمله مهاجم تلاش می‌کند دسترسی به خدمات شبکه

		برای کاربران مجاز ناممکن شود. این مقصود معمولاً با روش‌هایی نظیر ایجاد ترافیک مصنوعی برای کارگزار خدمت و یا قطع ارتباط عملی می‌شود.
deny	منع، ممانعت، انکار، رد، حاشا	
derived key	کلید برگرفته	در کاربردهای رمزنگاری برخی اوقات لازم است که طرف-های درگیر بر اساس کلید اصلی از پیش مشترک، یا کلمه عبور یا هسته اولیه، اقدام به تولید یک یا چند کلید مشترک با طول عمر کمتر نمایند. کلید(های) تولید شده را کلید برگرفته گویند.
DES (Data Encryption Standard)		یک رمز قالبی با طول قالب داده ۶۴ بیت و طول کلید ۵۶ بیت که در سال ۱۹۷۷ میلادی توسط اداره استاندارد ملی آمریکا(NBS) به عنوان استاندارد رمزنگاری اسناد غیر طبقه-بندی شده اعلام شد. با مطرح شدن حملات مختلف علیه این رمز، رمز *AES* جایگزین آن شد.
description logic	منطق توصیفی	
designated confirmer signature = confirmer signature	امضای تایید کننده	
deterministic	قطعی، یقینی	
deterministic encryption	رمزگذاریِ قطعی، رمزگذاری یقینی	رمزنگاری که در آن به ازای یک متن اصلی و کلید مشخص، همیشه فقط یک متن رمز مشخص حاصل می شود، مثل بیشتر رمزهای قالبی در سبک ECB. در مقابل Probabilistic Encryption
dictionary attack	حملهٔ واژه نامه‌ای	حمله جهت پیدا کردن گذرواژه. در این حمله دشمن با جمع آوری لغاتی که برای گذرواژه معمول هستند، یک واژه نامه از گذرواژه‌ها تهیه می‌کند. سپس با جستجوی تمام کلمات واژه‌نامه به سیستم حمله می‌کند.
dictionary based attack	حملهٔ مبتنی بر واژه نامه	
difference distribution table	جدول توزیع تفاضلات	
differential cryptanalysis	تحلیل تفاضلی	حمله ای از نوع سوم (حمله بر اساس متن اصلی منتخب) علیه رمزهای قالبی، در این حمله دشمن می‌کوشد تا رابطه محتملی میان تفاضل ورودی‌ها وتفاضل خروجی‌ها در هر دور رمز پیدا کند. با کنار هم گذاشتن این روابط احتمالی در دورهای متوالی رمز، تحلیلگر انتظار رابطه محتملی بین

		تفاضل ورودی و تفاضل ورودی به دور آخر رمز – به ازای زوج متن‌هایی با تفاضل ورودی مشخص- دارد. با این دانایی تحلیلگر می تواند به حدس تعدادی بیت از زیر کلید دور آخر بپردازد و بخشی از دور آخر را رمز گشایی کند، و در میان حدس‌ها کلیدی را به عنوان کلید صحیح بپذیرد که تفاضل مورد انتظار تحلیلگر را در داده‌های ورودی به دور آخر تا حدی نشان دهد.
differential power analysis attack (DPA)	حملهٔ تحلیل توان تفاضلی	نوعی حمله تحلیل توان پیشرفته. رجوع کنید به power analysis attack
Diffie-Hellman key exchange = Diffie-Hellman key agreement = exponential key exchange	پروتکل تبادل (مبادله) کلید دیفی- هلمن	پروتکلی برای تبادل امن کلید از طریق یک کانال نا امن، مبتنی بر دشواری حل مسئله لگاریتم گسسته.
diffusion	پراکنش	یکی از دو قاعده‌ای که شانون برای مقاوم کردن رمز پیشنهاد کرد. این قاعده بیان می کند که هر بیت متن اصلی و یا هر بیت کلید باید تعداد زیادی از بیت‌های متن رمز را تحت تاثیر قرار دهد. برای نیل به این هدف، از تبدیلاتی که خواص آماری متن اصلی را در طول متن رمز شده پراکنده کنند، استفاده می‌شود. جایگشت، یک نوع تبدیل با اثر پراکنش است. روش دیگر آشفته سازی (confusion) است.
digital	رقمی، دیجیتال	داده‌هایی که به صورت رقم (عموماً ارقام صفر و یک) هستند، داده‌های دیجیتال نامیده می‌شوند.
digital certificate	گواهینامه رقمی/دیجیتال	
digital envelope	پاکت رقمی	
digital evidence	گواه دیجیتالی/رقمی، شاهد دیجیتالی/رقمی	هر نوع اطلاعاتی که به صورت رقمی ذخیره یا مخابره می‌شود و از آن می‌توان در دادگاه به عنوان مدرک استفاده کرد.
digital ID	شناسهٔ رقمی/دیجیتال	
digital signature	امضای رقمی، امضای دیجیتال	مقداری که به متن ارسالی پیوست می شود و انتظار می‌رود همان ویژگی امضای معمولی را داشته باشد. یعنی هم ثابت کند پیام حتماً از طرف فرستنده مورد نظر است (authentication) و هم صحت پیام را تایید کند (integrity) ، ضمناً فرستنده نتواند بعداً متن و امضای خود را انکار کند(non-repudiation). مقدار امضا از اعمال تابع وابسته به کلید خصوصی شخص فرستنده بر روی متن ارسالی

تولید می شود.		
معادلات چندجمله ای با مجهولات صحیح.	معادله دیوفانتین	Diophantine equation
طرحی که در صورت رخداد یک خرابی سخت افزاری یا نرم افزاری یا تخریب امکانات در اثر سانحه، جهت بازیابی و بازسازی آنها ارائه می‌شود.	طرح بازیابی پس از سانحه	disaster recovery plan (DRP)
	طرد	discard
نوعی حملهٔ تحلیل ترافیک احتمالاتی برای تعیین تمام موجودیت‌هایی که با یک کاربر در ارتباطند؛ و نتیجه آن کاهش میزان گمنامی کاربر است.	حملهٔ افشاء	disclosure attack
	قطع اتصال	disconnection
مسئله یافتن مقدار x در معادلهٔ $b^x \equiv n \pmod m$، با داشتن مقادیر b، n، و m. تا کنون روش کارایی برای حل این مسئله پیدا نشده است و دشواری حل این مسئله مبنای طراحی تعدادی از الگوریتم‌های رمز قرار گرفته است.	مسئلهٔ لگاریتم گسسته	discrete logarithm problem
	کنترل دسترسی اختیاری، کنترل دسترسی احتیاطی	discretionary access control
یک رخداد برنامه ریزی نشده که باعث می شود کل سامانه یا یک برنامه کاربردی عمده، برای یک مدت زمان غیرقابل قبول از کار بیفتد (مانند قطع برق جزئی یا گسترده، قطع شبکه گسترده، یا تخریب تجهیزات و امکانات).	اختلال	disruption
الگوریتمی نظیر D که وظیفه‌اش تمیز دادن ورودی‌های نوع X از ورودیهای نوع Y است. به عبارت دیگر، تمایزگر موفق است اگر مقدار: $\left\|\Pr\{D(X)=1\}-\Pr\{D(Y)=1\}\right\|$ کمیتی غیر ناچیز باشد. معمولاً تمایزگر به عنوان ابزاری جهت تحلیل رمز بکار برده می شود.	تمایزگر	distinguisher
حمله‌ای که در آن تحلیل‌گر تلاش می کند یک دنباله تولید شده توسط الگوریتم رمز را با یک احتمال قابل قبول از یک دنباله تصادفی تمیز دهد.	حملهٔ تمایز	distinguishing attack
	شناسهٔ تمایز	distinguishing identifier
	محاسبات توزیع‌شده	distributed computing
حملات DoS ممکن است نفوذگر را به موفقیت کامل نرساند، مگر آنکه خطوط با پهنای باند بالا در اختیار داشته	حملهٔ منع سرویس توزیع‌شده	distributed denial of service(DDoS)

		باشد. در حملات DDoS از رایانه‌های پراکنده در سراسر اینترنت که توسط نفوذگر آلوده شده‌اند، برای حمله به هدف استفاده می‌شود.
divide and conquer	تقسیم وحل	گاهی با تقسیم یک مسئله بزرگ به قسمت‌های کوچک‌تر، حل مسائل کوچک‌تر راحت تر از حل کلی مسئله است. در بیشتر رمزها، ساختار کلی از کنار هم گذاشتن چند مولفه در کنار هم تشکیل شده است، که ممکن است این مولفه ها به تنهایی از مقاومت مطلوبی برخوردار نباشند. در صورتی که ترکیب مولفه‌ها به گونه‌ای باشد که امکان جداسازی و تحلیل برخی از این مولفه‌ها منجر به تحلیل کل رمز گردد، این ویژگی می‌تواند مبنای حملاتی قرار گیرد که حملات تقسیم و حل نامیده می‌شوند
DMZ→Demilitarized Zone		
DNS attack	حمله به DNS	انواع حملات با هدف از کار انداختن این خدمت.
DNS cache poisoning	مسموم کردن DNS	نام دیگری برای جعل DNS. به DNS spoofing رجوع شود.
DNS spoofing	جعل DNS	روشی جهت حمله به DNS، در این حمله یک کارگزارDNS جعلی با اطلاعات گمراه کننده به جای کارگزارDNS واقعی جا زده می‌شود.
DNS→Domain Name System		
document	سند	
doll code	کُد عروسک	یک سامانه رمز که در طول جنگ جهانی دوم برای تأمین اطلاعات مورد نیاز دولت ژاپن در باره موقعیت و حرکت کشتی‌های جنگی امریکا مورد استفاده قرار می‌گرفته است. در این سامانه از پیام‌های جعلی راجع به عروسک‌ها به منظور انتقال اطلاعات مورد نظر استفاده می‌شده است. مبدع این روش خانم Valvalee Dickinson یک حامی جدی ژاپن در طول جنگ بوده و مالک یک فروشگاه عروسک فروشی در شهر نیویورک بوده است.
domain name system (DNS)	سامانهٔ نام دامنه	
dominate	غلبه داشتن	گوئیم سطح امنیت S1 بر سطح امنیت S2 غلبه دارد، هرگاه در دسته‌بندی سلسله‌مراتبی، S1 بزرگتر یا برابر با S2 بوده و در طبقه‌بندی غیر سلسله‌مراتبی، S1 شامل S2 به عنوان یک

		زیرمجموعه باشد
doorknob rattling attack	حملهٔ دق الباب	در این حمله نفوذگر یک به یک رایانه‌ها را به قصد نفوذ می‌آزماید تا شاید یک درب قفل نشده بیابد.
DoS→Denial of Service Attack		
dot dot attack (..)	حملهٔ دو نقطه (..)	مهاجم با استفاده از مجوز دسترسی به یک پوشه، تلاش می‌کند به پوشه‌های دیگری خارج از محدوده مجاز، دسترسی یابد.
double encryption	رمزگذاری دوگانه	
DPA→Differential Power Analysis Attack		
DSA (Digital Signature Algorithm)		یک الگوریتم رمزنگاری نامتقارن که امضاء رقمی را به شکل یک زوج از اعداد بزرگ تولید می‌کند. این الگوریتم توسط اداره استاندارد ملی آمریکا به عنوان الگوریتم استاندارد امضاء رقمی معرفی شده است.
DSP→Digital Signal Processor		
DSS (Digital Signature System)		یک سامانه رمز برای تولید و بررسی امضاء رقمی بر مبنای DSA که توسط NIST در سال۱۹۹۱ به عنوان استاندارد امضاء رقمی اعلان شد. امنیت این امضاء مبتنی بر پیچیدگی حل مسئله لگاریتم گسسته است.
dual	دوگان	
dual encryption protocol (DEP)	پروتکل رمزگذاری دوگان	
dual-use certificate	گواهینامه دو منظوره	یک گواهی که برای هر دو کاربرد امضای دیجیتال و رمزنگاری داده‌ها صادر شده است.
due care	مراقبت الزامی	مراقبتی که مدیران و سازمان های آن‌ها وظیفه دارند برای امنیت اطلاعات در نظر بگیرند تا تضمین کنند که نوع کنترل، هزینه کنترل و استقرار کنترل برای سیستم مناسب باشد.
dummy message	پیام ساختگی	پیامی که حاوی هیچ اطلاعاتی نیست و به صورت تصادفی تولید شده است.
dumpster diving	آشغال گردی	
duplicate digital evidence	مدرک دیجیتال نسخهٔ دوّم	نسخه دوم یک بازتولید دقیق دیجیتالی از همه اشیاء داده ای درون یک قلم فیزیکی اصلی و رسانه مرتبط با آن.
duration	طول، مدت	
dynamic	پویا	

dynamic host configuration protocol (DHCP)	پروتکل پیکربندی میزبان پویا	پروتکلی که برای تخصیص آدرس های پروتکل اینترنت (IP) به همه گره‌های شبکه به کار می‌رود.
E		
easter egg	تخم مرغ عید	عملکرد پنهان در یک برنامه کاربردی، که هنگامی فعال می-شود که یک مجموعه دستورات و ضربات کلید غیرمستند و اغلب پیچیده وارد شوند. تخم مرغ های عید معمولاً برای نشان دادن افتخارات تیم تولید به کار می‌روند و قصد غیر مخرب دارند.
E-authentication→ electronic authentication		
eavesdropping	استراق سمع، شنود	
ECB→Electronic Codebook mode		
ECC→Error Correcting Code یا Elliptic Curve Cryptography		
ECDSA→Elliptic Curve DSA		
echo request	درخواست پژواک	
EDE→Encipher-Decipher-Encipher		
edit distance	فاصلهٔ ویرایشی	
effective	اثربخش، موثر	
effective key size	اندازه موثر کلید	
efficiency	کارآیی	
egress	حق یا مجوز خروج	
egress filtering	تصفیهٔ خروجی	فرآیند جلوگیری از عبور بسته‌های خارج شونده که به طور آشکار، آدرس‌های پروتکل اینترنت (IP) دروغین - مانند آدرس‌های مبدا از شبکه‌های داخلی - دارند.
electromagnetic analysis(EM) attack	حملهٔ تحلیل تشعشعات الکترومغناطیسی	دسته‌ای از حملات کانال جانبی که با استفاده از اندازه‌گیری تشعشعات الکترومغناطیسی دستگاه رمزنگاری سعی در یافتن مقادیر مخفی آن دارد.
electronic authentication (E-authentication)	احراز اصالت الکترونیکی	فرآیند اطمینان یافتن به هویت کاربران که به طور الکترونیکی به یک سامانه اطلاعاتی ارائه می‌شوند.
electronic cash	پول الکترونیکی	
electronic codebook operating mode (ECB)	سَبک کتابچه رمز	ساده‌ترین سبک به‌کارگیری رمزهای قالبی، که در آن متن اصلی به قطعات به طول مساوی تقسیم شده و قطعه‌ها به ترتیب وارد تابع رمزنگاری شده و قطعات رمز شده حاصل

		می‌شوند.
electronic coin	سکهٔ الکترونیکی	
electronic data interchange	مبادلهٔ الکترونیکی داده	
electronic signature	امضای الکترونیکی	
electronic wallet	کیف پول الکترونیکی	
ElGamal public-key encryption	رمزگذاری کلید همگانی الجمال	یک نوع سامانه رمزنگاری کلید همگانی مبتنی بر مسئله لگاریتم گسسته.
ElGamal signature scheme	طرح امضای الجمال	یک نوع امضای دیجیتال مبتنی بر الگوریتم رمز الجمال که امنیت آن بر سختی حل مسئله لگاریتم گسسته استوار است.
eligibility	مجاز بودن	
elliptic curve cryptography	رمزنگاری مبتنی بر خم بیضوی	یک نوع سامانه رمزنگاری کلید همگانی مبتنی بر ساختار جبری خم های بیضوی.
email	رایانامه	
email filtering	تصفیه رایانامه	
embedded system	سامانهٔ تعبیه شده، سامانه جاگذاری شده	
encapsulation	لفافه‌بندی	
encipher	رمزگذاری	تبدیل متن آشکار به متن رمز شده. در مقابلdecipher
encipher-decipher-encipher(EDE)		به کارگیری مکرر رمز قالبی جهت افزایش امنیت. اعمال رمزگشایی و رمزگذاری مربوط به یک رمز، ولی با کلیدهای جداگانه اعمال می‌شوند. مثال: DES سه گانه
enciphered	رمز شده	
encode	کدگذاری	
encoder	کدگذار	
encrypt	رمزگذاری	
encrypted	رمز شده	
encryption	رمزگذاری	در مقابل decryption
end to end	سرتاسر، انتها به انتها	
end to end encryption	رمزگذاری سرتاسری	
end to end security	امنیت سرتاسری	
end user	کاربر نهایی	
enemy	دشمن	کسی که مجاز به آگاهی از کلید و یا متن اصلی نیست، ولی با روش‌هایی سعی در فهمیدن پیام و یا پیدا کردن کلید و یا

		دخالت در ارتباط را دارد.
entity	هستار	هر دستگاه، سامانه یا واحد عملکردی مستقل
entrapment	دام گذاری	قرار دادن نقایص آشکار در یک سامانه پردازش داده، با هدف کشف تلاش‌های انجام شده برای نفوذ به سامانه یا گیج کردن یک نفوذگر در مورد انتخاب نقص مورد استفاده.
entropy	آنتروپی	متوسط اطلاعات موجود در هر نماد، متوسط ابهام موجود در هر نماد.
entry	مدخل، درایه	
ephemeral key	کلید موقت	کلیدی است که با توجه به نحوه تولید و اقتضائات امنیتی، تنها در یک جلسه یا اتصال مورد استفاده قرار می‌گیرد. عموماً به زوج کلیدهای همگانی-خصوصی که تنها در یک اجرا از پروتکل برقراری کلید استفاده می‌شوند، اطلاق می-گردد.
ephemeral secret	راز موقت	
erasure error	خطای با محل معین	خطای ناشی از ابهام در نماد دریافتی.
error correction code	کُد تصحیح خطا	
error detection code	کُد تشخیص خطا	دسته‌ای از کدهای کانال که تنها وقوع خطا را در دنباله دریافتی شناسایی می‌کنند، اما قادر به تصحیح خطا نیستند. مانند کدهای CRC و کدهای توازن.
escrow	امان سپاری	سند رسمی که نزد شخص سوم معتمدی به امانت گذاشته می شود و در صورت حصول شرایط مشخصی قابل اجرا و یا ابطال می‌گردد.
espionage	جاسوسی	
evaluation metric	معیار ارزیابی	
evasion attack	حملهٔ گریز	در این حمله، نفوذگر از تفاوت در تفسیر بسته توسط میزبان نهایی و سیستم تشخیص نفوذ یا دیواره آتش، سوء استفاده می‌کند. از این رو نفوذگر می‌کوشد به وسیله تکنیک‌های ویژه‌ای سیستم تشخیص نفوذ و دیواره آتش را فریب دهد تا بتواند بسته مخرب خود را از این سیستم‌های بازرسی عبور داده و به مقصد مورد نظر ارسال کند.
event	رویداد	
event driven	مبتنی بر رویداد، رویداد مبنا	
event logger	رویدادنگار	

event oriented	رویدادگرا	
exclusive OR (XOR)	یای انحصاری	عملگری روی بیت‌ها که حاصل آن برای بیت های یکسان برابر با صفر و برای بیت های ناهمسان یک است.
executive	اجرایی	
exhaustive key search attack	حملهٔ جستجوی فراگیر فضای کلید	حمله‌ای که در آن تمام حالات ممکن تا رسیدن به جواب آزمایش می‌شود. یعنی تمام مقادیر ممکن برای کلید آزمایش می‌شود تا کلید مربوط به یک یا چند زوج متن اصلی و رمز شده آن که در دسترس است، بدست آید. کران بالای امنیت یک سیستم رمز با تلاشی که جهت انجام این حمله انجام می‌شود، اندازه گیری می‌شود.
exhaustive search	جستجوی فراگیر	بررسی تمام حالت‌های ممکن تا رسیدن به جواب مسئله.
existential forgery	جعل وجودی	
expiry time	زمان انقضا	
exploit code	کد سوءاستفاده	
exposure	افشا	
F		
fabrication	جعل	افزودن اطلاعات
fabrication attack	حملهٔ جعل	حمله‌ای که در آن با وارد کردن داده‌های اضافی به سیستم، اعتبار داده‌ها را مختل می‌کند.
fair cryptosystem	سیستم رمز منصف	
fairness	انصاف	
false acceptance rate	نرخ پذیرش غلط	مقدار احتمال این‌که یک سیستم شناسایی، یک فرد را به طور نادرست شناسایی کند یا نتواند فردی غیر مجاز را از ورود به سیستم منع کند.
false negative	منفی غلط	۱. اخطاری که به نادرست وجود یک فعالیت بدخواهانه را ردّ می‌کند. ۲. نام دیگر خطای نوع اول در آزمون فرض آماری، ردّ فرض صفر، وقتی که درست باشد.
false positive	مثبت غلط	۱. اخطاری که به نادرست انجام یک فعالیت بدخواهانه را اعلام می کند. ۲. نام دیگر خطای نوع دوم در آزمون فرض آماری، قبول فرض صفر، وقتی نادرست باشد.
fault	عیب	عدم قابلیت سامانه، دستگاه، ... در انجام کار مورد نظر
fault analysis attack	حملهٔ تحلیل عیب	یکی از انواع حملات کانال جانبی که در آن با القای

		خطاهای عمدی و معین به دستگاه رمزنگاری، یک خروجی (متن رمز یا متن اصلی) خطادار تولید می‌شود. سپس با استفاده از خروجی‌های خطادار و نوع خطای القا شده، تحلیل گر سعی در یافتن کلید مخفی دستگاه تحت حمله دارد.
fault detection	عیب یابی	
federal information processing standards(FIPS)	استانداردهای پردازش اطلاعات فدرال	مجموعه‌ای از استانداردهای تدوین شده توسطNIST در حوزه امنیت فناوری اطلاعات
feedback	پسخورد	نمونه‌ای که از خروجی گرفته و به ورودی داده می شود. (جهت کنترل و یا ادامه کار سیستم)
Feistel construction	ساختار فَیستلی	روشی کلی برای طراحی رمزهای قالبی، در این روش قالب داده به دو زیرقالب تقسیم می شود. سپس زیرقالب اول توسط تابعی (وابسته به کلید) درهم ریخته و با زیرقالب دوم ترکیب می‌شود. پس از آن زیرقالب دوم توسط تابعی (وابسته به کلید) در هم ریخته و با زیرقالب اول ترکیب می‌شود. این کار به طور متوالی چند بار تکرار می‌شود. اگر به جای تقسیم قالب به دو زیرقالب، قالب داده به n زیرقالب تقسیم شود، به آن فَیستل مرتبه n گویند. رمز DES یک رمز فایستلی مرتبه ۲ است.
Fiat-Shamir identification protocol	پروتکل شناسایی فیات شامیر	
field	میدان	
file transfer protocol(FTP)	پروتکل انتقال پرونده	
filtering	تصفیه	
filtering router	مسیریاب تصفیه	
financial cryptography (FC)	رمزنگاری مالی	به کاربردن رمزنگاری در کاربردهایی که آسیب دیدن ساختار اطلاعاتی موجب خسارت مالی می‌شود.
fingerprint	اثرانگشت	
finite field	میدان متناهی	
finite state automaton	خودکاره حالت متناهی	
finite-state machine	ماشین حالت متناهی	
FIPS→Federal Information Processing Standards		
firewall	دیوار آتش، حفاظ	یک یا مجموعه‌ای از سامانه‌ها که سیاست کنترل دسترسی را بین شبکه ها اعمال می کنند.
firewall control proxy	نمایندهٔ کنترل حفاظ	مؤلفه‌ای که مدیریت یک درخواست توسط یک حفاظ را

کنترل می‌کند. نماینده کنترل حفاظ می‌تواند به حفاظ دستور دهد که درگاه‌های مشخصی را که مورد نیاز یک درخواست هستند باز نموده و با خاتمه درخواست، این درگاه‌ها را ببندد.		
محیط حفاظ، مجموعه‌ای از سیستم‌ها در یک نقطه بر روی شبکه هستند که با هم‌دیگر یک پیاده سازی حفاظ را تشکیل می‌دهند. محیط حفاظ می‌تواند از یک یا چندین دستگاه مانند حفاظ‌های متعدد، سیستم‌های تشخیص نفوذ و کارگزاران نماینده تشکیل شود.	محیط حفاظ	firewall environment
مجموعه قوانین حفاظ، جدولی از دستورات است که حفاظ، برای تعیین چگونگی مسیریابی بسته‌ها بین واسط‌ها به کار می‌برد. در مسیریاب ها، مجموعه قوانین می‌تواند فایلی باشد که مسیریاب هنگام تصمیم مسیریابی، آن را از بالا به پایین بررسی می‌کند.	مجموعه قوانین حفاظ	firewall ruleset
	سفت افزار	firmware
	تابع برازندگی	fitness function
	حملهٔ نقطه ثابت	fixed point attack
	حملهٔ زنجیره ای نقطه ثابت	fixed-point chaining attack
	ایراد، اشکال	flaw
	انعطاف پذیری	flexibility
لبریز کردن ظرفیت های یک منبع از طریق انجام اعمال پیاپی، به حدی که پاسخ‌گویی از توان آن خارج شده و از کار بیافتد.	سیلاب سازی	flooding
	حملهٔ سیلابی	flooding attack
	حملهٔ اعمال تاخیر	forced delay attack
	جعل	forgery
	صوری	formal
	رمز پیشرو	forward cipher
	حملهٔ جستجوی پیشرو	forward search attack
	محرمانگی پیشرو	forward secrecy
	امنیت پیشرو	forward security
	پیشرو	forward(1)
	باز ارسال	forward(2)
روشی برای حفظ محتوای داده که به هر نوع دستکاری حساس است و حتی می‌تواند محل دستکاری را کشف کند.	ته نقش نگاری شکننده، نشان گذاری شکننده	fragile watermark

fragment	تکه، قطعه	
fragmentation	تکه تکه کردن، تقطیع	
frame	قاب	
framework	چارچوب	
frequency analysis attack	حملهٔ تحلیل فراوانی حروف	در این حمله فراوانی حروف به صورت تَکی یا ترکیب چندتایی، در متن رمز محاسبه می‌شود و اطلاعات حاصل برای تحلیل الگوریتم های رمز کلاسیک مورد استفاده قرار می‌گیرد. تاریخ این تحلیل به دانشمند مسلمان «الکندی» در قرن سوم هجری می‌رسد.
frequency hopping	پرش فرکانسی	
frequency test	آزمون فراوانی	آزمونی آماری جهت بررسی میزان تصادفی بودن یک دنباله.
freshness	تازگی	اطمینان از تکراری نبودن پیام دریافتی.
FTP→File Transfer Protocol		
G		
gap of a sequence	شکاف دنباله	صفرهای متوالی در یک دنباله دودویی که بیت ماقبل و ما بعد آن یک باشد.
gate	دروازه، دریچه	
gateway	دروازه	
general deduction	استنباط کلی	
general number field sieve	غربال میدان اعداد عام	
generalization	تعمیم	
generator	مولد	
generic attack	حملهٔ عام	
global	سراسری	
goodness of fit test	آزمون زیبندگی	
gopher	گوفر	یک پروتکل در لایه کاربرد TCP/IP که برای توزیع، جستجو و بازیابی مستندات بر روی اینترنت طراحی شده و قبل از www استفاده می‌شده است.
Goppa code	کد گوپا	
graduated security	امنیت سطح بندی شده	یک سامانه امنیتی که بر مبنای تهدیدها، مخاطرات، فناوری موجود، سرویس‌های پشتیبان، ملاحظات زمان، نیروی انسانی و مسائل اقتصادی، چندین سطح (مثل پایین، متوسط، بالای) حفاظتی را فراهم می‌کند.

granularity	دانه‌بندی	بیان اندازه نسبی داده‌ها، برای مثال حفاظت اطلاعات در سطح پرونده به عنوان دانه‌بندی درشت و این حفاظت در سطح رکورد یا فیلد، به عنوان دانه‌بندی ظریف در نظر گرفته می‌شود.
gray hole attack	حملهٔ چاله خاکستری	یکی از انواع حملات منع خدمت که در آن بسته‌های یک مقصد خاص، به صورت انتخابی و یا تصادفی دور انداخته می‌شوند.
grey hat hacker	رخنه گر کلاه خاکستری	کسی که از روی کنجکاوی و بدون نیت خرابکارانه، بی-اجازه به سیستم‌های دیگران وارد می‌شود ولی خود را مقید می‌داند که به آنها آسیبی نرساند.
group key management protocol (GKMP)	پروتکل مدیریت کلید گروهی	
group signature	امضای گروهی	یک نوع امضا که در آن یک نفر از یک گروه به صورت گمنام از جانب دیگر اعضای گروه متنی را امضا می‌کند.
guard (system guard)	محافظ(سامانه محافظ)	سازوکاری که تبادل اطلاعات بین سامانه ها یا زیرسامانه‌های اطلاعاتی را محدود می‌کند.
guess and determine attack	حمله حدس وتعیین	یکی از حملات مطرح علیه رمزهای دنباله‌ای که در آن، تحلیل‌گر با حدس بخشی از فضای حالت اولیه الگوریتم و با توجه به روابط موجود و وابستگی سایر مقادیر به مقادیر حدس زده شده تلاش می‌کند تا سایر مقادیر نامعلوم را تعیین کند.
H		
hack	رخنه کردن، نفوذ کردن	توانایی و مهارت استفاده از روش‌های اکتشافی برای شناسایی و عبور از موانع امنیتی سامانه‌های رایانه‌ای.
hacker	رخنه گر،نفوذگر	
hacking	رخنه‌گری، نفوذگری	
Hadamard transform	تبدیل هادامارد	
hamming distance	فاصلهٔ همینگ	فاصله همینگ دو دنباله دودویی تعداد مکان‌هایی در دو دنباله است که مقادیر دو دنباله در آن مکان‌ها متفاوت‌اند.
hamming weight	وزن همینگ	تعداد یک ها در یک دنباله دودویی.
hand shaking	دست دادن	
handler	گرداننده	۱. نوعی برنامه که برای کنترل عوامل توزیع شده در شبکه در حملات منع سرویس توزیع شده به کار می‌رود. ۲. هم چنین به فردی که کارهای واکنشی در برابر حوادث

		را بر عهده دارد (به عنوان مدیر حوادث) نیز اطلاق می‌شود.
handoff	پاس‌کاری	
handshake	دستداد	
hard problem	مسئلهٔ سخت	به intractable problem مراجعه شود.
hard-code	کد سخت	نرم افزاری برای وارد و ثابت کردن داده ها (در یک کد منبع) به نحوی که داده‌ها به راحتی قابل تغییر نباشند.
hardening	مستحکم سازی	اقداماتی که جهت امن‌سازی بعضی میزبان‌های خاص که به دلیل وظایف‌شان خارج از ناحیه بی طرف(DMZ) قرار دارند، مثل کارگزاران وب، کارگزاران پست الکترونیکی، کارگزاران DNS و میزبان سنگرها صورت می گیرد.
hardware-oriented	سخت افزار- گرا	
hash function	تابع چکیده ساز	تابعی که طول ورودی آن دلخواه و طول خروجی آن ثابت است. از ویژگی‌های این توابع می توان به یک طرفه بودن، وابستگی خروجی به تمامی بیت‌های ورودی و بدون برخورد بودن اشاره کرد. یکی از مهمترین کاربردهای این توابع در تولید امضای دیجیتال است.
header	سرآیند	
heuristic security	امنیت تجربی	یک روش مبتنی بر تجربیات گذشته برای بهبود پایداری و تأمین امنیت سامانه‌ها در برابر حملات جدید.
hiding	پنهان سازی	روشی برای مقابله با حملات تحلیل توانی و حملات تحلیل تشعشعات الکترومغناطیسی
high assurance guard (HAG)	محافظ با اطمینان بالا	یک دستگاه حفاظتی با مرز محصور که دسترسی بین یک شبکه محلی و یک شبکه خارجی را با درجه اطمینان بالا کنترل می‌کند.
high impact system	سامانهٔ پر تأثیر	یک سامانه که بروز هرگونه نقصان در هر یک از اهداف امنیتی محرمانگی، یکپارچگی و یا قابلیت دسترسی، می تواند منجر به آسیب‌های جدی به آن گردد.
hijacking	سرقت، ربودن	
histogram	نمودار ستونی	
HMAC→Hash-based Message Authentication Code		
homogeneous	همگن	
homomorphism property	ویژگی هم ریختی	

honeynet	شبکهٔ تله عسل	یک شبکه غیر واقعی که رفتار یک شبکه واقعی را تقلید کرده و با مشغول کردن نفوذگر به خود او را از شبکه اصلی دور نگه می‌دارد تا مسئولین شبکه بتوانند فعالیت او را مشاهده و تدابیر دفاعی مناسب اتخاذ کنند.
honeypot	تلهٔ ظرف عسل	تله‌ای که با اغفال مهاجم او را به هدفی غیر واقعی مشغول کرده و از دسترسی به سامانه های حیاتی دور می‌دارد و به مدیران سامانه امکان مشاهده فعالیت های مهاجم و اتخاذ سیاستهای اجرایی مناسب را می‌دهد.
hook	قلاب	
host impersonation attack /server spoofing attack	حملهٔ جعل کارگزار	حمله‌ای که در آن مهاجم خود را به جای کارگزار واقعی جا زده و با کاربران ارتباط برقرار می‌کند. اگر کاربر نتواند کارگزار جعلی را از کارگزار واقعی تشخیص دهد، درخواست ارتباط را پذیرفته و داده‌های محرمانه خود را در اختیار مهاجم قرار می‌دهد
host to host	میزبان–به–میزبان	
host to LAN	میزبان به شبکهٔمحلی	
host-based	مبتنی بر میزبان	
hot site	پایگاه آماده‌باش	امکانات پردازش داده کاملاً عملیاتی در خارج از پایگاه، که برای استفاده در صورت رخداد یک سانحه با سخت افزار و نرم افزار تجهیز شده باشد.
hub	ناف	یک وسیله ارتباطی که نقطه اتصال مشترک برای تجهیزات یک شبکه ارتباطات رایانه‌ای است.
hybrid encryption	رمزگذاری ترکیبی	کاربردی از رمزنگاری که در آن از ترکیب حداقل دو الگوریتم رمز، به ویژه ترکیبی از رمزهای متقارن و نامتقارن استفاده می شود.
hyper link	اَبراتصال	
hyper text	ابرمتن	
hyperexponential	اَبر نمایی	تابعی به صورت $e^{g(n)}$ که مرتبه $g(n)$ از n بزرگتر باشد، مثل e^{n^2}
hypertext markup language (HTML)	زبان نشانه گذاری اَبرمتنی (زنگام)	.
I		
ICMP attacks (Internet Control Message Protocol attacks)	حملات ICMP	ICMP بخشی از پروتکل TCP/IP است که مسئول ارسال پیام‌های خطا و تأمین روش‌هایی برای آزمودن شبکه‌های IP

		است. سوء استفاده از این پروتکل مبنای چندین حمله قرار گرفته است. به ICMP fingerprinting،ICMP flood، ICMP sweep مراجعه کنید.
ICMP fingerprinting	انگشت نگاری از ICMP	این حمله از ICMP برای مشخص کردن سیستم عاملی که روی یک میزبان در حال اجراست، استفاده می‌کند.
ICMP flood	سیلاب سازی ICMP	همان حمله اسمورف است. به Smurf attack رجوع کنید.
ICMP sweep = ping sweep	جاروب ICMP	روشی برای مشخص کردن این که کدام میزبان‌ها در یک شبکه فعال هستند.
ID Code	کد شناسه	
IDEA		یک نوع الگوریتم رمزنگاری قالبی.
ideal security	امنیت ایده آل	
identification	شناسایی، تعیین هویت	
identity	شناسه	
IETF→Internet Engineering Task Force		
impact	تأثیر	میزان آسیبی که انتظار می رود در نتیجهٔ افشای غیرمجاز اطلاعات، تغییر غیرمجاز اطلاعات، تخریب اطلاعات، از دست رفتن اطلاعات و یا دسترس پذیری سیستم اطلاعاتی برای افراد غیر مجاز پدید آید.
Impersonation attack	حملهٔ جعل هویت	حمله‌ای که در آن مهاجم خود را به جای یکی از طرفین درگیر در ارتباط جا زده و سعی در فریب طرف دیگر دارد. اطلاعات لازم برای شکل‌گیری این حمله معمولاً با استراق سمع پیام‌های مربوط به چندین ارتباط متوالی اخیر به دست می‌آیند.
implementation	پیاده سازی	
implication	دلالت	
implicit	ضمنی	
impossible differential attack	حملهٔ تفاضل ناممکن	حمله‌ای که در آن یک تفاضل ناممکن بین مقادیر میانی رمز به ازای تعدادی زوج متن انتخابی پیدا می‌شود. سپس کلیدهایی که به چنین تفاضلی منجر شوند، از مجموعه حدس ها خارج می شوند. این عمل تا جایی که مقداری جز کلید اصلی در مجموعه حدس ها نماند، ادامه می یابد. کلید باقی مانده نهایی، همان کلید رمز است.
incident	حادثه	نقض یا نقض قریب‌الوقوع خط مشی‌های امنیتی رایانه، خط

		مشی‌های کاربری مورد پذیرش، یا استانداردهای امنیتی رایانه.
incoercibility	عدم اجبار	از الزامات امنیتی برای رای دهندگان، تا حمله کننده نتواند اقدام به اجبار رای دهنده و یا خرید رای وی کند.
IND-CCA→ Indistinguishable Chosen-Ciphertext Attack		
IND-CCA2→ Indistinguishable Adaptive Chosen-Ciphertext Attack		
indistinguishability	تمایزناپذیری	
indistinguishable adaptive chosen-ciphertext attack (IND-CCA2)	حملهٔ متن رمز منتخب وفقی تمایز ناپذیر	
indistinguishable chosen-ciphertext attack (IND-CCA)	حملهٔ متن رمز منتخب تمایز ناپذیر	
infected attachment	پیوستِ آلوده	
information	اطلاعات	
information dispersal algorithm (IDA)	الگوریتم انتشار اطلاعات	رخدادی که عملاً یا به طور بالقوه، محرمانگی، صحت یا دسترس پذیری یک سیستم اطلاعاتی و یا اطلاعات ذخیره شده توسط فرآیندهای سیستم را به خطر می‌اندازد، یا موجب نقض خط مشی های امنیتی، رویه های امنیتی و یا خط مشی های کاربری مورد قبول می‌شود.
information hiding	پنهان‌سازی اطلاعات	
information leakage	نشت اطلاعات	
information sharing	تسهیم اطلاعات، به اشتراک گذاری اطلاعات	
information system	سامانهٔ اطلاعات	
information system security officer (ISSO)	مامور امنیت سامانه اطلاعات	
information technology (IT)	فناوری اطلاعات (فا)	
information warfare	جنگِ اطلاعات	
infrastructure	زیرساخت	
ingress filtering	تصفیهٔ ورودی	فرآیند جلوگیری از ورود بسته‌هایی که آدرس های IP نادرست، مانند آدرس های منبع رزرو شده، دارند.

inheritance	ارث‌بری	
initial value (IV) =initialization vector	مقدار اوّلیه	در برخی کاربردهای رمز، مقداری برای شروع عمل رمزنگاری نیاز است که به آن مقدار اولیه گویند. لزومی ندارد که مقدار اولیه محرمانه باشد، ولی باید تصادفی بوده و قبلاً استفاده نشده باشد.
initialization	مقداردهی اوّلیه	
insecurity	ناامنی	
insertion attack	حملهٔ درج	یکی از روش‌های متداول برای سوء استفاده از شبکه‌های بی-سیم است که در آن عملکرد سازوکارهای امنیتی موجود با وارد کردن و کاربرد مخفیانه تجهیزات غیرمجاز مختل می-گردد.
insider attack	حملهٔ داخلی	حمله‌ای توسط یک کارمند یا یک فرد قابل اعتماد و یا به طور کلی فردی با امکان دسترسی بیش از حدّ معمول.
inspection	بازرسی	
integer counter mode(ICM)= Counter mode	سبک شمارنده	
integer factorization	تجزیه به عوامل صحیح	
integral cryptanalysis	تحلیل یکپارچه	حمله‌ای علیه رمزهای قالبی با ساختار شبکه جانشینی و جایگشت(SPN)
integration	یکپارچه‌سازی	
integrity	یکپارچگی، تمامیت	یکی از اهداف امنیت، یعنی اطمینان از این‌که چیزی به متن ارسالی، اضافه و یا از آن کم نشده باشد و یا هیچ‌گونه تغییری در آن رخ نداده باشد.
integrity check value (ICV)	مقدار بررسی تمامیت، معیار تمامیت	
inter host communication	ارتباط بین میزبان	
inter realm	درون قلمرویی	
interaction	تعامل	
interactive	تعاملی	
interception	دستبرد	
interface	واسط	
interleaving	میان‌گذاری، درهم بافی	
interleaving attack	حملهٔ درهم بافی	
internet	اینترنت	

internet engineering task force (IETF)		یک انجمن عمومی برای تدوین استانداردها دراینترنت.
internet service provider (ISP)	ارائه کنندهٔ خدمات اینترنتی	
interoperability	قابلیت همکاری	
interpolation	درون‌یابی	
interpolation attack	حملهٔ درون‌یابی	نوعی حمله جبری علیه رمزهای قالبی. متن رمز شده هر رمزی قابل بیان به صورت یک چند جمله‌ای بر حسب متن اصلی است که ضرایب چندجمله‌ای توابع مشخصی از کلید هستند. اگر تعداد جملات چند جمله‌ای کم باشد، می‌توان به جای بدست آوردن مقدار کلید، ضرایب چندجمله‌ای را یافت. به تحلیل رمز با چنین روشی، حمله درونیابی گفته می شود.
interruption	وقفه	
intractable problem = hard problem	مسئله سرکش	مسئله‌ای که حل آن در زمان چند جمله ای، توسط ماشین تورینگ قطعی ممکن نباشد.
intruder	نفوذگر	
intrusion	نفوذ	
intrusion detection	تشخیص‌نفوذ	
intrusion detection system (IDS)	سامانهٔ تشخیص نفوذ	سامانه‌ای که با تحلیل ترافیک ورودی و خروجی شبکه یا تحلیل تقاضاها سعی در شناسایی فعالیت های نفوذگر می-نماید و در صورت تشخیص نفوذ، مسئول شبکه را مطلع می-کند یا واکنش خاصی انجام می دهد.
invasive attack	حملهٔ تجاوزی	حمله‌ای که با دست‌کاری (Tamper) در دستگاه رمزنگاری سعی در یافتن مقادیر مخفی دارد. این حمله که از قوی ترین حملات کانال جانبی به شمار می رود، عموماً با خارج کردن دستگاه رمزنگاری از بسته بندی و اتصال پروب به سیگنال-های داخلی تراشه آغاز می‌شود.
inversion attack	حملهٔ وارون‌سازی	حمله‌ای علیه رمزهای دنباله‌ای.
invertible	وارون‌پذیر	
involution	خودوارون	تبدیلی که معکوسش با خودش برابر است یعنی $f(f(x)) = x$.
IP security (IPsec)	امنیت IP	یک پروتکل استاندارد موسسه IEEE که قابلیت های امنیتی را در لایه پروتکل اینترنت (IP) ارتباطات فراهم می کند.
IP spoofing	جعل IP	حمله‌ای که در آن حمله کننده با جایگزین کردن IP یک

		فرد معتمد در سرآیند بسته های خود، قربانی را متقاعد می-کند که پیام را از سوی فرد مورد اعتماد دریافت می کند.
irreducible polynomial	چندجمله‌ای تحویل‌ناپذیر، چندجمله‌ای ساده نشدنی	
isomorphic property	ویژگی یک‌ریختی	
iterated	مکرر، تکراری	
IT-related risk	مخاطره مرتبط با IT	
IV→Initial Value		
J		
jammer	اخلال‌گر	
jamming	اختلال	
jitter	لرزه	
join - request	درخواست الحاق	
K		
Kerberos authentication protocol	پروتکل احراز اصالت کربروس	یک پروتکل احراز اصالت شناخته شده در شبکه که بر رمزنگاری متقارن و استفاده از یک نهاد ثالث مورد اعتماد مبتنی است. این پروتکل بر اساس پروتکل "نیدهام-شرودر" بنا نهاده شده است، با این تفاوت که در آن فرض شده که ساعت تمام ایستگاه‌های شبکه دقیقا با هم تنظیم شده‌اند.
Kerckhoffs' assumption	فرض کرشهف	فرض کرشهف: تمام الگوریتم‌های رمزنگاری آشکار و همگانی هستند و تنها کلیدهای رمز، مخفی و محرمانه هستند.
kernel	هسته	
key	کلید	توابع رمز معمولاً به جز متن اصلی پارامتر دیگری به عنوان ورودی می‌گیرند، این پارامتر روند رمزنگاری را کنترل می کند و در بین تعداد زیادی از تبدیل‌های موجود بین فضای متون اصلی و فضای متون رمز، یک تبدیل را انتخاب می-کند.
key agreement	توافق کلید	
key clustering attack	حملهٔ خوشه بندی کلید	نوعی حمله بر روی رمزهای قالبی.
key distribution	توزیع کلید	
key distribution Center(KDC)	مرکز توزیع کلید	
key escrow	امانسپاری کلید	
key establishment	برقراری کلید، استقرار کلید	
key exchange	مبادلهٔ کلید	

key expansion	توسیع کلید	استخراج کلیدِ دورها از کلید اصلی
key generation material	موّاد تولید کلید	اعداد تصادفی، شبه تصادفی و پارامترهای رمزنگاری که در تولید کلید به‌کاربرده می شوند.
key loader	بارکنندهٔ کلید	یک واحد داخلی که قادر است حداقل یک کلید رمزنگاری یا مؤلفه کلید را به صورت متن ساده یا رمزشده ذخیره نموده و در صورت درخواست، آن را به واحد رمزنگاری انتقال دهد.
key logger	ثبت کننده صفحه کلید	
key management	مدیریت کلید	مجموعه فعالیت‌هایی که برای اداره کلیدهای رمزنگاری و دیگر پارامترهای امنیتی مربوط (مثل گذرواژه‌ها و مقادیر اولیه) در طول عمر کلید شامل تولید، نگهداری، توزیع و انهدام آنها صورت می‌گیرد.
key notarization	ثبت رسمی کلید	
key pair	زوج کلید	
key recovery	بازیابی کلید	
key revocation	ابطال کلید، فسخ کلید	
key schedule	تولید زیر کلید	
key translation center (KTC)	مرکز ترجمه کلید	
key transport	انتقال کلید	انتقال امن کلید رمزنگاری از یک طرف ارتباط به طرف مقابل.
key whitening	سفید کردن کلید	روشی برای افزایش امنیت رمز قالبی، که در چند مرحله داده با بخشی از کلید ترکیب می شود (قبل از دور اول و بعد از دور آخر رمزگذاری).
key wrap	پوشش کلید، لفافه کلید	روشی برای رمزنگاری کلیدها (به همراه اطلاعات مربوط به صحت آن‌ها) که هم حفظ محرمانگی و هم حفظ صحت را با استفاده از یک الگوریتم کلید متقارن فراهم می‌کند.
key-only attack	حمله فقط بر اساس کلید	
keyspace	فضای کلید	
keystream	دنبالهٔ کلید اجرایی	
keystroke monitoring	پایش صفحه کلید	فرآیندی که برای مشاهده یا ذخیره ضربات وارده به صفحه کلید توسط کاربر و هم چنین پاسخ های رایانه در خلال یک جلسه تعاملی به کار می رود و بر مبنای آن می‌توان اطلاعات وارد شده توسط کاربر را استنتاج نمود.
kleptography	سرقت نگاری	بررسی این‌که یک سامانه رمز چگونه طراحی شود تا به طور

		ناخودآگاه و بدون اطلاع کاربر، اطلاعاتی از کلید را به طراح نشت دهد
knapsack problem	مسئلهٔ کوله پشتی	
knowledge	دانش، دانایی	
known IV attack	حملهٔ مبتنی بر بردار اوّلیه معلوم	
known plaintext attack	حمله مبتنی بر متن اصلی معلوم	در این حمله، تعدادی متن اصلی و متن رمز شده متناظر با آن‌ها در اختیار است. به این نوع حمله «حمله نوع دوم» نیز گفته می شود.
L		
LAN →Local Area Network		
latin square	مربع لاتین	یک مربع لاتین از مرتبه n عبارتست از یک ماتریس مربع n× n که عناصر آن دقیقًا از n نماد متمایز تشکیل شده است، به طوری‌که هرنماد در هر سطر و ستون فقط یک‌بار ظاهر شود .
lattice	مشبّکه	
layer	لایه	
LC→Linear Cryptanalysis		
leased line	خط استیجاری	
least privilege	حداقل مجوز	اعطای تنها دسترسی‌هایی به کاربران که آن‌ها برای انجام وظایف خود نیاز دارند.
legitimate	قانونی	
letter frequency	فراوانی حرف	تعداد تکرار یک حرف در یک متن
level of significance	سطح اهمیت	
lexicographical order= dictionary order	ترتیب قاموسی	
LFSR→ Linear Feedback Shift Register		
life time	عمر، طول عمر	
lightweight cryptography	رمزنگاری سُبُک	شاخه‌ای از رمزنگاری که در آن طرح‌ها و پروتکل‌های رمزنگاری با هدف به کارگیری در محیط‌های دارای منابع محاسباتی و ذخیره سازی محدود مورد بررسی قرار می-گیرند.
linear approximation attack	حملهٔ تقریب خطی	
linear complexity	پیچیدگی خطی	

linear complexity test	آزمون پیچیدگی خطی	آزمونی که در آن با تعیین طول کوچکترین ثبات انتقال خطی که می‌تواند یک دنباله مشخص و محدود دودویی را تولید کند، رفتار آن دنباله مورد بررسی قرار می‌گیرد.
linear consistency attack	حملهٔ سازگاری خطی	
linear cryptanalysis (LC)	تحلیل خطی	حمله‌ای از نوع دوم (حمله متن اصلی معلوم) علیه رمزهای قالبی، در این روش رابطه‌ای خطی با احتمال (نسبتا) بالا بین بیت های ورودی و خروجی هر دور رمز استخراج می شود. با کنار هم گذاشتن روابط تمام دورها به جز دور آخر، رابطه خطی محتملی بین بیت‌های ورودی به رمز و بیت‌های ورودی به دور آخر تشکیل می شود. از طرفی با حدس زدن تعدادی از بیتهای زیر کلید دور آخر، می توان قسمتی از دور آخر رمز را رمزگشایی کرده وبیتهای مورد نیاز در ورودی به دور آخر را بدست آورد. حال می توان رابطه خطی محتملی را که بین بیت های ورودی به رمز و بیتهای ورودی به دور آخر بدست آمده است را بررسی کرد. در میان کلیدهای حدس زده شده کلیدی به عنوان کلید صحیح پذیرفته می‌شود که رابطه خطی مذکور برای کسر قابل توجهی از متن‌ها صدق کند.
linear feedback shift register (LFSR)	ثبات انتقال با پس‌خورد خطی	آرایه‌ای خطی (بردار) با درایه‌هایی که معمولا با مقادیر صفر یا یک پر شده اند. در هر نوبت مقادیر درایه‌ها یکی به جلو انتقال می‌یابد و مقدار درایه آخر توسط حاصل ترکیب خطی درایه‌های دیگر مقداردهی می‌شود. به این ترکیب خطی از درایه‌های دیگر که درایه آخر را مقدار دهی می‌کند، پس‌خورد خطی گفته می شود.
linear sequential circuit approximation (LSCA)	تقریب مدار ترتیبی خطی	
linear syndrome attack	حملهٔ همرفت خطی	
linear transformation	تبدیل خطی	یک تبدیل خطی بین دو فضای برداری U و V تابعی است که در شرایط زیر صدق می‌کند: 1. $\forall v_1, v_2 \in V : T(v_1 + v_2) = T(v_1) + T(v_2)$ 2. $\forall v \in V, \alpha \in R : T(\alpha v) = \alpha T(v)$
linearization	خطی سازی	
linguistic steganography	نهان‌نگاری زبان شناختی	
link	پیوند، یال	

link analysis	تحلیل پیوند	
liveness (principal liveness)	حاضر بودن	در پروتکل‌های امنیتی، به مفهوم حضور واقعی فرد در روند اجرای پروتکل است.
load	بار	
load balancing	تعدیل بار، توازن بار	
loadable modules	پیمانه‌های قابل بارگذاری	
local area network (LAN)	شبکهٔ محلی	
local area network (LAN)	شبکهٔ داخلی، شبکهٔ محلی	
local registration authority (LRA)	مجوز ثبت محلی	
log	رویدادنگار، رخداد نما	
Log off =Log out	ثبت خروج	
Log on = Log in	ثبت ورود	
logging	رویدادنگاری، رخدادنگاری	
logic bomb	بمب منطقی	یک قطعه کد پنهانی در داخل یک برنامه مجاز که تحت شرایط خاصی (مثلا وقوع یک تاریخ مشخص) فعال شده و شروع به عملیات تخریبی می کند.
long term	طولانی مدت	
look up table	جدول مبنا	
loop	حلقه	
loose source routing	مسیریابی غیردقیق منبع	
low impact system	سامانهٔ کم تأثیر	یک سامانه اطلاعاتی که در آن، به هر سه هدف امنیتی (یعنی محرمانگی، صحت و دسترس پذیری) یک مقدار تأثیر گذاری پایین با توجه به استاندارد FIPS 199 اختصاص یافته است.

M

MAC→ Message Authentication Code		
macro payment	پرداخت کلان	
macro virus	ویروس کلان	ویروسی که خود را به اسناد متصل می‌کند و از قابلیت‌های برنامه نویسی ماکروی برنامه کاربردی سند برای اجرا و انتشار خود استفاده می کند.
mailbox	نامه‌دان	
maintenance	نگهداری	
malicious software	نرم افزار مخرب	

malleability	شکل پذیری	یک ویژگی ناخواسته در بعضی سیستم‌های رمزنگاری (کلید همگانی)، وقتی دشمن بتواند یک متن رمز را به یک متن رمز دیگر تبدیل کند به طوری که متن اصلی مربوط به متن رمز دوم، تابع مشخصی از متن اصلی مربوط به متن رمز اول باشد.
malware = malicious software	بدافزار	نرم‌افزاری که برای مقاصد سوء، تولید و بکار گرفته می‌شود.
man-in-the-middle attack(MITM)	حملهٔ فرد در میانه	این نوع حمله، حمله‌ای فعال است که در آن دشمن مستقلا با دو طرف ارتباط برقرار و طوری عمل می‌کند که طرفین ارتباط گمان کنند که از طریق یک کانال امن در حال ارتباطند. در حالی که همه مکالمات توسط دشمن تحت کنترل است.
manipulation	دست‌کاری	
manipulation detection code	کد تشخیص دست‌کاری	به توضیح واژهٔ modification detection code مراجعه شود.
many to one	چند به یک	
mapping	نگاشت	
MARS		یک رمز قالبی که یکی از ۵ نامزد منتخب برای AES بوده است. این سیستم دارای قالب‌های ۱۲۸ بیتی و طول کلید متفاوت بین ۱۲۴۸–۱۲۸ بیت است.
mask	پوشانه، نقاب	
masking	پوشش‌گذاری، نقاب گذاری	روشی برای مقابله با حملات توانی و حملات تشعشعات الکترومغناطیسی که با تصادفی سازی مقادیر میانی الگوریتم سعی در غیر همبسته کردن مقادیر توان مصرفی (یا مقادیر تشعشعات الکترومغناطیسی) با داده پردازش شده دارد.
masquerader	رخ پوش، نقابدار	کاربر غیرمجاز
masquerading	رخ پوشی، نقاب‌گذاری	مترادف Spoofing، تلاش مهاجم برای ورود به یک سامانه اطلاعاتی از طریق این‌که خود را یک کاربر مجاز وانمود کند (جا بزند).
mass mail (MM)	سیل نامه، توده نامه	ارسال حجم انبوه رایانامه از طریق پست الکترونیکی.
master key	شاه کلید، کلید اصلی	کلیدی که دارای عمر طولانی‌تری نسبت به کلیدهای جلسه است.
matching	تطابق	
Maurer's universal statistical test	آزمون آماری فراگیر مارور	آزمونی آماری برای بررسی رفتار دنباله‌های دودویی که در سال ۱۹۹۲ ارائه شد. ادعا شده است که توسط این آزمون می‌توان هر رفتار غیر تصادفی یک دنباله را به لحاظ آماری

		تشخیص داد.
McEliece cryptosystem	سامانه رمز مَک اِلیس	یک سامانه رمزنگاری کلید همگانی مبتنی برنظریه کدینگ که امنیت آن مبتنی بر دشواری کدگشایی یک کد خطی بدون اطلاع از ساختار ماتریس مولد آن است. کلید این رمز با استفاده از ماتریس مولد یک کد خطی تولید می شود. در طرح اولیه این سامانه از کدهای گوپا استفاده شده بود. از این طرح می‌توان سامانه رمزنگاری کلید همگانی، کلید خصوصی و همچنین امضای دیجیتال استخراج نمود.
MD5(Message Digest5)		یک نوع الگوریتم چکیده ساز از خانواده MD
MDC→Modification Detection Code		
MDS code	کد MDS	یک کد تصحیح خطا که بیشترین فاصله همینگ ممکن بین کلمات آن وجود داشته باشد. مانند کدهای RS
MD-strengthening→ Merkle-Damgard Strengthening		
measure of roughness	معیار ناهمواری	
mechanism	ساز و کار	
meet in the middle attack	حمله ملاقات در میانه	حمله‌ای شبیه حمله روز تولد، با این تفاوت که در حمله روز تولد در دامنه تابع به دنبال دو عضو هستیم که تابع به ازای آن دو دارای مقدار یکسانی باشد، در حالی که در این حمله، در دامنه و برد ترکیب دو تابع، به دنبال عضوی هستیم که تبدیل مستقیم تابع اول مساوی با معکوس تبدیل تابع دوم شود. به عبارتی در محل ترکیب دو تابع ملاقات داشته باشیم.
memory-resident virus	ویروس مقیم در حافظه	نوعی ویروس که به عنوان بخشی از یک برنامه سیستمی در حافظه اصلی رایانه مقیم می‌شود و از این نقطه هر برنامه‌ای را که اجرا می شود آلوده می‌سازد.
mere semantics	معنا شناسی محض	
merge	ادغام شدن	ترکیب دو فایل اطلاعات به نحوی که فایل نتیجه از همان ساختار فایل‌های ترکیب شده برخوردار باشد.
Merkle-Damgard construction	ساختار مرکل دمگارد	روشی برای طراحی توابع چکیده ساز، که در آن داده ورودی به تعدادی قطعه با طول ثابت و مشخص تقسیم و سپس یک تابع فشرده ساز به طور مکرر روی قطعات حاصل و خروجی مرحله قبل اعمال می شود. نهایتاً خروجی حاصل از مرحله آخر به عنوان خروجی تابع در نظر گرفته می‌شود.

Merkle-Damgard strengthening= MD-strengthening= Length Padding	مقاوم سازی مرکل-دمگارد، مقاوم سازی MD	یک نوع دنباله‌زنی در طراحی توابع در هم ساز که موجب ایجاد مقاومت در برابر برخورد می شود، در این روش، طول ورودی در بیت های دنباله قرار می‌گیرد.
Mersenne number	عدد مرسن	عددی به صورت $M_n= 2^n -1$ که در آن، n عددی طبیعی است.
mesh	تورینه	
message authentication	احراز اصالت پیام	
message authentication code (MAC)	کد احراز اصالت پیام	چکیده وابسته به کلید یک پیام، که به پیام پیوست می‌شود و صحت پیام و اصالت فرستنده را اثبات می‌کند.
message concealing	مخفی سازی پیام	
message digest	چکیده پیام	
message integrity	یکپارچگی پیام، تمامیت پیام	
message integrity code (MIC)	کد یکپارچگی پیام، کد تمامیت پیام	
meta data	فراداده	
metamorphic virus	ویروس دگردیس	این ویروس علاوه بر تغییر ظاهر خود بعد از هر بار الوده سازی، رفتار خود را نیز عوض می‌کند. و بنابراین تشخیص آن مشکل است.
metropolitan area network	شبکهٔ شهری	
micro payment	پرداخت خرد	در مقابل macro payment.
million instrument per second (MIPS)	میلیون دستورالعمل در ثانیه	واحد اندازه گیری برای مقایسه سرعت ریزپردازنده‌ها.
MIME(Multipurpose Internet Mail Extension)	گسترش چندمنظوره رایانامه	گسترشی بر رایانامه که در آن می‌توان علاوه بر متن، از محتوای چند رسانه‌ای (نظیر تصویر، صوت، و فیلم) نیز استفاده کرد.
MIPS→Million Instrument Per Second		
MIPS-year	MIPS-سال	تعداد گام‌های پردازش شده در یک سال با فرض اجرای یک میلیون دستورالعمل در ثانیه.
misfeasor	کاربر خاطی	
misnamed	بد نام	روشی برای پنهان کردن محتوای یک فایل با تغییر دادن نام فایل به یک موجودیت بی‌خطر یا تغییر پسوند آن به یک نوع فایل دیگر، که بررسی کننده را وادار می‌کند تا فایل را به وسیله امضای فایل – و نه پسوند آن – شناسایی کند.
misrouting attack	حملهٔ مسیردهی غلط	این نوع حمله یکی از خطرناک‌ترین حملات علیه ساختار

اینترنت است و به وسیله مسیریاب‌هایی به وجود می‌آید که با اهداف مخرب، بسته‌های اطلاعات را در جهت‌های نادرست هدایت می‌کنند. این نوع حملات می‌توانند سبب بروز مشکلاتی نظیر ازدحام در شبکه، منع خدمت، تقطیع شبکه و افت کارآیی شبکه گردند.		
	فقدان	miss
این حمله با پیروی از ایده حمله ملاقات در میانه، روش نسبتاً کارآمدی برای یافتن تفاضل های ناممکن در الگوریتم رمز پیشنهاد می‌دهد. حمله عبارت است از یافتن دو واقعه (حالت) با احتمال یک، که هیچ گاه یکدیگر را در میانه ملاقات نکنند.	حملهٔ فقدان در میانه	miss-in-the-middle attack
	زمان ماموریت	mission time
	ماموریت پذیری	missionability
	تشخیص سوءاستفاده	misuse detection
		MITM →Man In The Middle attack
حمله‌ای که توسط شخصی به نام Mitnick پایه‌گذاری شد، و اساس آن سوء استفاده از یک آسیب‌پذیری در پیاده‌سازی پروتکل TCP بود.	حملهٔ میت‌نیک	Mitnick attack
روشی برای ایجاد یک کانال ناشناس است که در آن با استفاده از ابزار رمزنگاری سعی می‌شود که ارتباط بین ورودی‌ها و خروجی‌های کانال حذف و گمنامی کاربران تامین شود.	شبکهٔ آمیزنده، شبکهٔ مخلوط	mix net
	آمیختن، مخلوط‌سازی	mixing
	رمز مخلوط‌ساز	mixing cipher
	سبک	mode
دسته‌ای از توابع درهم ساز بدون کلید، مانند: MD5، SHA-1.	کد تشخیص تغییر	modification detection code (MDC)
	پیمانه	module
	پایش، نظارت	monitoring
	جانشینی تک الفبایی	monoalphabetic substitution
	تک جمله‌ای	monomial
	یک‌نوا	monotone
	m- رجعت پذیر	m-resilient

m-sequence = maximum length sequence	دنباله بیشینه	دنباله‌ای با دوره تناوب $2^n - 1$ که توسط یک ثبات با پس-خورد خطی به طول n تولید شده است.
multilevel caching	نهان‌سازی چند سطحی	
multiple encryption	رمزگذاری چندگانه	ترکیب چند الگوریتم رمز.
multisignature	چندامضایی	
mutual authentication	احراز اصالت دوسویه/متقابل	پروتکل احراز اصالتی که در آن هر یک از طرفین ارتباط، اصالت خود را به فرد مقابل اثبات می‌کند. در مقابل unilateral authentication
N		
national institute of standard and technology(NIST)	موسسه ملی استاندارد و فناوری	این موسسه مسئولیت تدوین استانداردهای امنیت رایانه‌ای و روش‌های ارزیابی برنامه های کاربردی منفک از وزارت دفاع امریکا را بر عهده دارد. فعالیت‌های این موسسه علاوه بر تدوین استانداردها، شامل تحقیقات نیز می شود.
navigation	ناوش، ناوبری	
need to know principle = principle of least privilege	اصل دانستن در حد نیاز، اصل حداقل اجازه دسترسی	قاعده‌ای در کنترل دسترسی که بر مبنای آن به هر فردی فقط باید آن‌قدر اجازه (دسترسی به منابع) داد که بتواند وظایف خاص خودش را انجام دهد.
negligible	ناچیز	
NESSIE(New European Schemes for Signature, Integrity and Encryption)		یک پروژه پژوهشی اروپایی در سالهای ۲۰۰۳-۲۰۰۰ برای شناسایی بهترین الگوریتم‌ها و پروتکل‌های امنیتی رمزنگاری.
net-mask	نقاب شبکه	
network	شبکه	
network access server (NAS)	کارگزار دسترسی شبکه	
network address translate (NAT)	ترجمهٔ نشانی شبکه	فرآیند تغییر اطلاعات مربوط به آدرس شبکه در سرآیند بستهٔ دیتاگرام در یک ابزار مسیر دهی. هدف از این فرآیند، نگاشت یک فضای آدرس به فضایی دیگر است، و اغلب برای شبکه‌هایی که تعداد محدودی IP مجاز دارند استفاده می‌شود.
network file system (NFS)	سامانهٔ فایل‌های شبکه	نوعی سامانهٔ فایل که امکان به اشتراک گذاردن فایل‌ها، چاپگرها، و دیگر منابع را میان اجزای مختلف شبکه فراهم می‌کند.
network IDS base	سامانه تشخیص نفوذ شبکه مبنا	

network information center (NIC)	مرکز اطلاعات شبکه (ماش)	
network interface	واسط شبکه	
network scanner	پویشگر شبکه	
network security	امنیت شبکه	
network time protocol(NTP)	پروتکل همزمانی شبکه	پروتکلی برای هماهنگ کردن ساعت و تاریخ بین اجزای مختلف شبکه
network weaving	شبکه بافی	روشی برای نفوذ که در آن از شبکه‌های رایانه‌ای مختلف برای دستیابی به یک سامانه پردازش داده، ضمن اجتناب از شناخته شدن یا ردیابی شدن، استفاده می شود.
NFSR→Non-Linear Feedback Shift Register		
Niederreiter encryption scheme	طرح رمزگذاری نیدِرِیتر	یک سامانه رمز مبتنی بر نظریه کدگذاری که امنیت آن مبتنی بر دشواری کدگشایی یک کد خطی بدون اطلاع از ساختار بررسی درستی آن است. این رمز به عنوان دوگان سیستم رمز مک‌اِلیس شناخته شده است، زیرا از ماتریس بررسی توازن برای ساخت کلید استفاده می کند.
NIST→National Institute of Standard and Technology		
node	گره	
noise	نوفه، اغتشاش	سیگنال نامطلوب و ناخواسته که به لحاظ ماهیت تصادفی قابل حذف توسط فیلتر نیست.
Nonce	تک‌شمار، عدد یکبار مصرف	عدد یا رشته عددی که تنها یک بار تولید و مورد استفاده قرار می‌گیرد و کاربرد آن درمقابله با حمله تکرار در پروتکل‌های رمزنگاری است.
non-interactive	غیر تعاملی	
non-invasive attack	حمله غیرتجاوزی	حمله‌ای که بدون تغییر در مشخصات دستگاه رمزنگاری و در حالی که دستگاه رمزنگاری به فعالیت خود ادامه می دهد، سعی در یافتن مقادیر مخفی آن را دارد. این دسته از حملات، عموماً حملات کانال جانبی نامیده می شوند. حمله تحلیل توانی و حمله تحلیل زمانی نمونه‌هائی از این دسته حملات هستند.
non-linear feedback shift register (NFSR)	ثبات انتقال با پس‌خورد غیرخطی	همانند ثبات انتقال خطی (LFSR) با این تفاوت که تابع پس‌خورد، تابعی غیرخطی است.
nonlinearity	غیر خطی بودن	
non-malicious	غیرمخرب	

non-malleable	شکل ناپذیر	یک طرح رمز کلید همگانی، شکل ناپذیر نامیده می شود، هرگاه به ازای متن رمز داده شده C1، تولید یک متن رمز شده دیگر مانند C2 به گونه ای که متن های اصلی متناظر آن‌ها دارای ارتباط معلومی باشند، از نظر محاسباتی مشکل باشد.
nonpersistent	ناماندگار	
non-repudiation	انکار ناپذیری	
notarization	رسمی سازی	
notary	دفتر ثبت رسمی	
NP Problems = Nondeterministic Polynomial Problems	مسائل از نوع NP ، مسائل از درجه سختی فراتر از چندجمله‌ای	مسائلی که بر روی یک ماشین تورینگ قطعی در یک زمان چندجمله‌ای قابل حل نباشند. ولی روی یک ماشین تورینگ غیرقطعی دارای راه حلی با زمان چندجمله‌ای باشند.
NP-complete	NP- تمام	
NP-hard	NP–سخت	
NSA(national security agency)	آژانس امنیت ملی آمریکا	
null	پوچ	
O		
OAEP→ Optimal Asymmetric Encryption Padding		
obligation	الزام	
OFB→Output Feedback mode		
off-line	برون خط	
omnipresent	همه جا حاضر	
one-time password	گذرواژه یک‌بارمصرف	گذرواژه‌ای که فقط یک بار قابل استفاده است.
one-time-pad cipher	رمز با کلید یک‌بار مصرف	یک نوع الگوریتم رمز، که در آن متن رمز از جمع متن اولیه و دنباله تصادفی کلید تولید می‌شود. در این رمز طول کلید به اندازه طول متن است و فقط یک‌بار مصرف می‌شود. این سیستم رمز دارای امنیت کامل است.
one-way function	تابع یک طرفه	تابعی که محاسبه آن سر راست و راحت است، ولی محاسبه معکوس آن از لحاظ محاسباتی بسیار سخت است.
on-line	بر خط	
on-to	پوشا	
ontology	هستان شناسی	

Opcode (operand code)	کد عملگر	مخفف Operation Code، کدی در زبان ماشین که نوع عملی را که ریزپردازنده باید انجام دهد، مشخص می‌کند.
operand	عملوند	
operating mode	سَبک به‌کارگیری، سبک اجرایی	معمولاً رمزهای قالبی به نحوه‌های متفاوتی در عمل مورد استفاده قرار می‌گیرند. نحوه بکار گیری رمز قالبی در عمل رمزنگاری را سَبک اجرایی آن گویند. از جمله سَبک‌های اجرایی می‌توان به ECB(Electronic Codebook) ، CFB(Cipher Feedback mode)، OFB(Output Feedback mode) اشاره کرد.
opponent	دشمن	
Optimal Asymmetric Encryption Padding (OAEP)	لایی‌گذاری بهینه رمز نامتقارن	یک روش لایی‌گذاری با امنیت قابل اثبات برای رمز کردن پیام که معمولاً برای سیستم رمز RSA به کار می‌رود و از یک پیشگوی تصادفی بهره می‌برد.
oracle	پیشگو، سروش	
order	مرتبه، درجه	
outage	قطع ارتباط	
output feedback mode(OFB)	سَبک پس‌خورد خروجی	یکی از سبک‌های به‌کار گیری رمز قالبی که با آن امکان به‌کارگیری یک رمز قالبی، با عملکردی مشابه با رمزهای دنباله‌ای فراهم می‌شود. این سبک دارای مزایایی نظیر امنیت بالا، انتشار خطای محدود و ایمنی در برابر حملهٔ واژه‌نامه است.
over flow	سر ریز	
overdefined	بیش تعریف	وقتی در یک دستگاه معادلات، تعداد معادلات از تعداد مجهولات بیشتر باشد.
overhead	سربار	
overlap	هم‌پوشانی	
P		
package	بسته	
packet	بستک	
packet sniffer	دیده‌بان بسته ها، شنودگر بسته‌ها	نرم افزاری که ترافیک شبکه را مشاهده و ذخیره می‌کند.
padding	دنباله زدن، لایی گذاری	به عمل اضافه کردن دنباله‌ای تصادفی از بیت‌ها که معنی مشخصی ندارند، ولی با اهداف مشخص - نظیر تکمیل طول قالب در رمزهای قالبی و یا تصادفی نمودن متن اصلی در

		رمزهای کلید همگانی- اضافه می شوند، دنباله‌زنی گوییم.
pager	پی‌جو	
parity	توازن	
passcode	گذر کد، کد عبور	
passive attack	حمله غیرفعال	حمله‌ای که دشمن در متن و محتوای پیام دست نمی برد و تنها به شنود اکتفا می کند.
passkey	کلید عبور	
passphrase	عبارت عبور	
password	کلمهٔ عبور، گذر واژه	
patch	وصله	نرم‌افزار اصلاحی.
patent	امتیاز، حق انحصاری	
P-Box→Permutation Box		
peer to peer	نظیر به نظیر، همتا به همتا	
PEM (privacy enhanced mail)		استاندارد ارائه شده توسطIETF برای امن‌سازی رایانامه با استفاده از رمزنگاری کلید همگانی.
pending	بلاتکلیف، معلق	
penetration	نفوذ	
penetration test	آزمون نفوذپذیری	آزمودن عملکردهای یک سامانهٔ پردازش داده برای پیدا کردن روشی برای نقض امنیت آن. طی این آزمون ارزیاب‌ها تلاش می کنند با فریب دادن سامانه امنیتی، راه‌های نفوذ به لایه‌های مختلف منابع سامانه را کشف کنند.
perfect forward secrecy	امنیت پیشرو کامل	یکی از ویژگی‌های پروتکل‌های تبادل کلید در سامانه رمز کلید عمومی که کاربران را از ایمن بودن سامانه در مقابل خطر کشف رمز حتی پس از کشف کلید خصوصی توسط دشمن مطمئن می‌سازد. یعنی با افشای یک کلید خصوصی طولانی مدت که در پروتکل تبادل کلید استفاده شده، امنیت هیچ یک از نشست‌های قبلی به خطر نیافتد.
perfectly secure system	سامانهٔ کاملاً امن	یک سامانه رمز را کاملاً امن گویند، هرگاه متن رمز شده مستقل از متن اصلی باشد.
performance	کارایی	
permutation	جایگشت	
permutation box (P-Box)	جعبهٔ جایگشت	
persistent	ماندگار	

personal area network (PAN)	شبکه شخصی	
personal digital assistant (PDA)	دستیار رقمی شخصی	
personal identification number (PIN)	شماره شناسایی شخصی	
pervasive computing environment	محیط محاسباتی گسترده	با گسترش روز افزون حجم داده‌ها، برای کنترل و حفاظت از آن‌ها، توزیع داده انجام می‌شود. یکی از انواع محیط های توزیع شده، محیط محاسبات فراگیر است.
PGP (pretty good privacy)		یک بسته نرم‌افزاری برای تامین امنیت رایانامه‌ها است که در سال ۱۹۹۱ ارائه شد و با یک ساختار بسیار ساده کاربری، تمام امکانات شامل تدوین نامه های خصوصی(رمز شده)، احراز اصالت، امضای دیجیتالی و حتی فشرده‌سازی اطلاعات را به صورت یک‌جا عرضه کرده است.
phishing attack	حملهٔ صیادی	روشی برای سرقت اطلاعات است که هدف آن اغفال کاربران به منظور دزدیدن اطلاعات خصوصی آن ها اعم از نام کاربری، کلمه عبور و ... می باشد. در یک حمله صیادی کاربر ترغیب می شود تا بر روی لینکی که در نامه الکترونیکی وجود دارد کلیک نماید. لینک بدکار، کاربر را به یک صفحه غیر قانونی هدایت می کند که ظاهرش شبیه سایت معتبر است. این صفحه، یک صفحه صیادی می باشد. صفحه صیادی از کاربر درخواست می کند تا اطلاعات شخصی اش مانند کلمه عبور مربوط به بانک یا اطلاعات کارت اعتباری اش را در صفحه وارد نماید و آن ها را ارسال نماید.
physical attack	حملهٔ فیزیکی	یکی از انواع حملات که در آن دستگاه رمزنگاری در اختیار دشمن قرار می گیرد.
Ping (packet internet groper)	پینگ	ابزاری در شبکه برای آزمودن قابل دسترس بودن، سرعت و واسط‌های یک مسیر ویژه از طریق آدرس IP
PKCS→ Public-Key Cryptography Standard		
PKI→ Public Key Infrastructure		
plaintext	متن اصلی	متن ورودی به تابع رمزنگاری و یا متن خروجی از تابع رمزگشایی.
platform for privacy preference project(P3P)	بستره توصیف اولویت‌های حریم خصوصی	یک قالب کلی برای توصیف خط مشی حفظ حریم خصوصی در پایگاه‌های اینترنتی تا سایت های مختلف، خط مشی حفظ حریم خصوصی خود را با ساختار یکسانی ارائه

		کنند.
plausible deniability	انکارپذیری باورکردنی	
Playfair cipher	رمز پِلِیفر	از انواع سیستم‌های رمز دو حرفی که در قالب جدولی ۵×۵ رمزنگاری را انجام می‌دهد.
PN sequence→ Pseudorandom Number Sequence		
point of present (pop)	بودگاه	
point of sale (PoS)	پایانه فروش	
policy	خط مشی	
policy description language (PDL)	زبان توصیف خط مشی	!
Pollard p-1 method	روش p-1 پلارد	یکی از الگوریتم‌های تجزیه برای دسته خاصی از اعداد مرکب.
Pollard Rho method	روش رو پلارد	روشی برای تجزیه یک عدد مرکب بزرگ و یا یافتن لگاریتم گسسته .
poly alphabetic	چندالفبایی	
polyalphabetic substitution	جانشینی چند الفبایی	
polymorphic virus	ویروس چندچهره	ویروسی که با هر بار آلوده سازی فایل‌ها ظاهر خود را عوض کرده و بنابراین تشخیص آن با مقایسه با یک نمونه قبل، غیر ممکن است.
polynomial	چندجمله‌ای	
polynomial time	زمان چندجمله‌ای	
port	درگاه	
port scanning	پویشِ درگاه	ارسال یک پیام به هر درگاه شبکه قربانی و دریافت جوابی که نشان می‌دهد که آیا درگاه باز و در نتیجه برای حمله مناسب است یا خیر؟
PoS→point of sale		
potential impact	تأثیر بالقوه	تاثیری که از دست‌دادن محرمانگی، صحت یا دسترس پذیری می تواند داشته باشد که به صورت اثر مضر ، اثر مضر جدی و یا اثر شدید یا فاجعه آمیز دسته بندی می شود.
power analysis attack	حملهٔ تحلیل توان	نوعی از حملات کانال جانبی که با اندازه گیری مقادیر توان مصرفی دستگاه رمزنگاری، سعی در یافتن مقادیر مخفی آن دارد.
p-problems = polynomial problems	مسائل از نوع چندجمله ای	مسائلی که در زمان چند جمله‌ای قابل حل هستند.

preamble	مقدمه	
precision	دقّت	
precursor	پیش‌آگهی	نشانه‌ای که یک مهاجم قبل از اقدام به وارد کردن یک آسیب، ممکن است منتشر کند.
preimage attack	حمله پیش تصویر	
preimage resistance	مقاومت در برابر پیش تصویر	همان ویژگی یک طرفه بودن است. یعنی با دانستن خروجی تابع، پیدا کردن یک ورودی که به این خروجی منجر شود، غیر ممکن باشد.
pre-paid payment	پیش پرداخت	
pre-play attack	حملهٔ پیش- اجرا	حمله‌ای علیه پروتکل‌های شناسایی هویت.
preprocess	پیش پردازش	
preshared key	کلیدِ از پیش مشترک	
primality test	آزمون اوّل بودن	آزمونی که اول یا مرکب بودن یک عدد را بررسی می کند.
primary key	کلید اوّلیه	
primitive polynomial	چندجمله‌ای اوّلیه	چندجمله‌ای $f(x)$ با درجه n در $F_2[x]$ اولیه نامیده می شود، هرگاه f در $F_2[x]$ ساده نشدنی بوده، $x^{2^n-1}+1$ را عاد کند، ولی به ازای هر عامل d از 2^n-1 ، x^d+1 را عاد نکند.
priority	اولویت، حق‌تقدم	
privacy	حریم خصوصی	
private key	کلید خصوصی	در سیستم رمزنگاری کلید همگانی از دو کلید استفاده می شود، کلیدی که مختص کاربر و محرمانه است، کلید خصوصی نامیده می شود.
private key cryptosystem	سامانه رمزنگاری کلید خصوصی	همان سیستم رمزنگاری متقارن است که در آن کلید بین فرستنده و گیرنده مشترک است.
private network	شبکهٔ خصوصی	شبکه‌ای که از رایانه‌ها و خطوط ارتباطی خصوصی یک شرکت تشکیل شده است.
PRNG→ Pseudorandom Number Generator		
proactive security	امنیتِ پویا	
probabilistic algorithm	الگوریتم تصادفی	
probabilistic encryption	رمز تصادفی	سامانه رمزی که به ازای یک متن اصلی و یک کلید مشخص، در هر بار رمزنگاری، متن رمزی متفاوت تولید می کند. مثل استفاده از سبک CBC در رمز قالبی.
probabilistic model	مدل احتمالاتی	

probabilistic public-key encryption	رمزِ کلید همگانی احتمالاتی	مزیتی در بعضی از سامانه‌های رمز کلید همگانی که یک پیام در هر بار اجرای الگوریتم به متن‌های متفاوتی رمز شود (سامانه رمز RSA فاقد این ویژگی است، اما مک‌اِلیس و الجمال دارای این ویژگی هستند.)
probabilistic signature scheme (PSS)	شمای امضای احتمالاتی	
procedure	رویه	
process	فرایند	
product cipher	رمزِ ترکیبی، رمزِ ضربی	یک نوع رمز قالبی که در آن با تکرار تعدادی اعمال به نام دور سعی می شود خواص پراکُنش و آشفتگی در رمز به طور کافی برآورده شود. هر دور ممکن است به تنهایی امنیت نداشته باشد، ولی تکرار آنها، امنیت کافی را تامین می‌کند. مفهوم رمز ضربی از مقاله شانون گرفته شده است.
profile	نمایه	
propagation criterion	معیار انتشار	گوییم تابع بولی f معیار انتشار از مرتبه k را برآورده می-سازد، هرگاه تغییر هر زیر مجموعه حداکثر k عضوی از بیت‌های ورودی تابع، منجر به تغییر خروجی تابع با احتمال $\frac{1}{2}$ شود.
protection	حفاظت	
protocol	پروتکل	
provable security	امنیت قابل اثبات	یک سامانه رمزنگاری دارای امنیت قابل اثبات است، اگر بتوان ثابت کرد که سختی شکستن آن رمز معادل سختی حل یک مسئله مشکل (مثل تجزیه اعداد بزرگ) است.
prover	اثبات کننده	کسی که باید ادعایی را ثابت کند.
proxy server	پیشکار	
proxy signature	امضای وکالتی	
pseudo attack	شبه حمله	حمله ای علیه توابع درهم ساز
pseudo collision	شبه برخورد	
pseudo-Mersenne primes	اعداد اوّل شبه مرسن	اعداد اول به صورت $p= 2^m - k$ که k در بازه $0 < \|k\| < 2^{\lfloor m/2 \rfloor}$ باشد.
pseudonym	نام مستعار	
pseudoprime	شبه اوّل	
pseudorandom	شبه تصادفی	
pseudo-random number generator (PRNG)	موّلد اعداد شبه تصادفی	

public directory	فهرست راهنمای همگانی	محلی در شبکه که آدرس و کلید همگانی کاربران را درخود جای داده است.
public key	کلیدِ همگانی	
public key cipher	رمز کلیدِ همگانی	
public key Infrastructure (PKI)	زیر ساختِ کلید همگانی	نهادی زیربنایی که با تولید، نگهداری، مدیریت و تصدیق اصالت کلید عمومی افراد و دیگر خدمات مربوط، شرایط لازم برای استفاده از فناوری‌های مبتنی بر رمزنگاری کلید همگانی را فراهم می کند.
public-key cryptography standards (PKCS):	استانداردهای رمزنگاری کلید همگانی	مجموعه‌ای از استانداردهای رمزنگاری با موضوع کلید همگانی که توسط موسسه RSA منتشر می شود.
purge	پاکسازی	پاکسازی داده ها به طوری که با روش‌های آزمایشگاهی قابل بازیابی نباشند.
quantum cryptography	رمزنگاری کوانتومی	
quartet	چهارتایی	
query	پرسمان	
R		
Rabin public-key encryption	رمزگذاری کلید همگانی رابین	نوعی سیستم رمزنگاری کلید همگانی که امنیت آن مبتنی بر دشواری تجزیه اعداد صحیح بزرگ است.
radio frequency identification tag (RFID tag)	برچسب شناسایی بسامد رادیوئی	برچسب‌هایی که بدون تماس هستند و با ورود شخص به محل مورد نظر توسط مقصد شناسائی می‌شوند.
rainbow table	جدولِ رنگین کمان	یک جدول درستی که برای بازیابی مقدار یک گذرواژه از روی مقدار چکیده آن به کار می رود. این جدول با برقراری مصالحه زمان و حافظه محاسبه وارون تابع چکیده ساز را تا حدی تسهیل می‌کند.
random	تصادفی	
random attack	حملهٔ تصادفی	حمله‌ای علیه توابع چکیده‌ساز که مستقل از الگوریتم است. در این حمله، دشمن یک پیام تصادفی را انتخاب می نماید و امیدوار است که مقدار چکیده پیام او برابر با مقدار چکیده یک پیام حقیقی باشد.
random number generator	مولّد اعداد تصادفی	
random oracle	پیشگوی تصادفی، سروش تصادفی	در رمزنگاری، پیشگو به کسی گفته می‌شود که برای هر پرسش یک پاسخ تصادفی از دامنه خروجی به طور یکنواخت انتخاب می‌کند. در حقیقت فرآیندی که هر پرسش ممکن را به یک پاسخ تصادفی از دامنه خروجی

		نگاشت می کند.
randomness	تصادفی بودن	
randomness test	آزمون تصادفی بودن	
RC6		یک سامانه رمزنگاری قالبی، این رمز یکی از پنج کاندید راه یافته به مرحله نهایی انتخاب AES بود.
r-collision	r–برخورد	وجود r ورودی که دارای خروجی یکسان باشند.
reactive	واکنشی	
real time	بی‌درنگ	به سیستم‌هایی گفته می شود که تاخیر ندارند و بلافاصله به درخواست رسیده، خدمات می دهند. برای مثال سیستم‌های رمز دنباله‌ای، بلادرنگ هستند، زیرا هر بیت بلافاصله رمز می‌شود. در مقابل در سیستم رمز قالبی بیت‌ها باید منتظر بیت-های دیگر شوند تا قالب کامل شده و سپس عمل رمز نگاری صورت گیرد.
realm	قلمرو، ناحیه	
receipt-freeness	بدون رسید بودن	از الزامات امنیتی برای طرح‌های رای گیری الکترونیکی است که در صورت برآورده شدنِ آن، رای دهندگان قادر به تولید یا اخذ مدرک یا رسیدی برای اثبات محتوای رای خود به سایرین نخواهند بود.
reciprocal polynomial	چندجمله ای معکوسه	
rectangular attack	حمله مستطیلی	حمله‌ای علیه رمزهای قالبی، ارتقاء یافته حمله بومرنگ
redundancy	افزونگی	
reflection attack	حملهٔ بازتاب	حمله‌ای در پروتکل‌های امنیتی که در آن فرد متخاصم، با باز ارسال پیام فرد مقابل به خود او به نحو حساب شده، او را فریب داده و هدف امنیتی پروتکل را نقض می کند.
regional authority (RA)	مراکز مجاز منطقه‌ای	
rekeying	توزیع مجدد کلید	
related key	کلید مرتبط	
related-key attack	حملهٔ کلید مرتبط	گاهی رابطه‌ای معلوم بین دو کلید رمزنگاری باعث نشت اطلاعات بین متن اصلی و متن‌های رمز شده می شود که تحلیل‌گر از آن استفاده می کند.
reliability	قابلیت اطمینان	
reliable	مطمئن	
relinearization	خطی سازی تکراری	
remailer	نامه پراکن	نوعی کارگزار که به کمک آن می‌توان رایانامه‌های فراوانی

را به صورت ناشناس در اینترنت پخش کرد		
عمل تصحیح یک آسیب پذیری یا حذف یک تهدید. سه نوع ترمیم ممکن عبارتند از: نصب وصله، تغییر تنظیمات پیکربندی، یا حذف یک برنامه نرم افزاری نصب شده.	ترمیم	remediation
یک نوع حمله به پروتکل های مورد استفاده در شبکه که در آن یک پیام معتبر با هدف سوء توسط نفوذگر تکرار می شود.	حملهٔ تکرار	replay attack
پایگاه داده‌ای که حاوی اطلاعات و داده‌های مربوط به گواهی‌ها است.	مخزن	repository
هرگاه G گروهی دوری و $g_1,g_2,..,g_n$ ، k مولد متمایز از G و h عضوی دلخواه در G باشد، n–تایی $(a_1,a_2,..,a_n)$ را یک نمایش از h نسبت به پایه مرتب $(g_1,g_2,..,g_n)$ در G نامیم، هرگاه $h=g_1^{a_1}g_2^{a_2}..g_n^{a_n}$ باشد. مسئله نمایش، یافتن یک نمایش از یک عنصر داده شده در G است. این مسئله در واقع تعمیمی از مسئله لگاریتم گسسته است.	مسالهٔ نمایش	representation problem
	مرتبهٔ رجعت پذیری	resiliency order
	توابع رجعت پذیر	resilient function
	اتلاف منبع، هدر دادن منبع	resource exhaustion
عبارتی که برای توصیه های مورد استفاده در اینترنت به کار می‌رود.		RFCs (Request For Comments)
		RFID Tag→ Radio Frequency Identification Tag
نام اولیه الگوریتم رمز AES ، پیش از انتخاب شدن به عنوان الگوریتم رمز استاندارد.		Rijndael
	ریسک، مخاطره	risk
		RNG→ Random Number Generator
	مقاوم بودن	robustness
در زیر ساخت کلید همگانی سلسله مراتبی به بالاترین سطح از مراکز صدور گواهی گفته می‌شود.	مرکز صدور گواهی ریشه	root CA
مجموعه‌ای از ابزارها که توسط رخنه‌گرها برای نفوذ به یک سامانه و بدست آوردن دسترسی در حد مدیر سیستم به یک رایانه یا یک شبکه مورد استفاده قرار می‌گیرد.	رخنه افزار	rootkit
	چرخش	rotation
	دور	round

round key	کلیدِ دور	
router audit tool(RAT)	ابزار ممیزی مسیریاب	مرتبط با محصول CISCO، ابزاری که تنظیمات را با تنظیمات معیار مقایسه کرده و در صورت نقصان، دستوراتی را برای تصحیح اشکالات بیان می‌دارد.
RSA algorithm	الگوریتم RSA	یک سیستم رمزنگاری کلید عمومی که امنیت آن بر دشواری تجزیه اعداد بزرگ بنا شده است.
run (of a sequence)	ردیف	بیت های یکسان متوالی در یک دنباله که با بیت ما قبل و ما بعد خود متفاوت باشند.
run test	آزمون ردیف	آزمونی آماری جهت بررسی میزان تصادفی بودن یک دنباله.
run time	زمانِ اجرا	
running key	کلیدِ اجرایی	
S		
S/MIME (Secure/Multipurose Internet Mail Extentions)		پروتکلی جهت افزودن خدمات امنیتی نظیر امضای دیجیتال و رمزنگاری به رایانامه در MIME
SAC→Strict Avalanche Criterion		
safe prime	عدد اوّل ایمن	یک عدد اول به شکل ۲p+۱ که در آن p نیز یک عدد اول است. مانند اعداد ۵، ۷، ۱۱، ۲۳، ۴۷، ...
safeguard	ایمن‌داشت	هر معیار یا کنترل حفاظتی که برای برآورده ساختن نیازهای امنیتی تعریف شده برای یک سامانه اطلاعاتی (مانند حفظ محرمانگی، تضمین صحت و تداوم دسترس پذیری) توصیه می‌شود. این نوع حافظت ها می‌توانند ویژگی‌های امنیتی سخت‌افزارها و نرم‌افزارها، رویه‌های اجرایی، شیوه‌های پاسخگویی، کنترل‌های دسترسی، محدودیت‌های مدیریتی، امنیت کارکنان، ساختارهای فیزیکی، نواحی و تجهیزات سازمان را شامل شوند اما تنها به این موارد محدود نمی‌باشند.
safety	ایمنی	ایمنی مخابره داده به معنای جلوگیری از خطاهای تصادفی است و با روش‌های کدگذاری کانال حاصل می‌شود، درحالی که امنیت مخابره به معنای جلوگیری از دریافت و یا دستکاری غیر مجاز عمدی است، که با روش‌های رمزنگاری تامین می‌شود.
salt	نمک، چاشنی	مقداری تصادفی که همراه با یک مقدار امنیتی مثل گذرواژه استفاده می‌شود تا میزان تصادفی بودن آن را افزایش دهد. مثلا هنگام ثبت گذرواژه‌ها، برای آنکه چکیده دو گذرواژه

یکسان، یکی نشود، ابتدا به آن نمک اضافه می‌کنند و بعد چکیده آن را محاسبه و ثبت می‌کنند.		
	نمک‌زنی	salting
فرآیند حذف اطلاعات از رسانه به طوری که بازیابی اطلاعات ممکن نباشد. این کار شامل حذف تمام برچسب ها، نشان گذاری‌ها و رویدادنگاری فعالیت‌ها می‌شود.	پاکسازی	sanitization
هرگاه فرم نرمال فصلی(conjunctive normal form) یک تابع بولی داده شده باشد، تصمیم بر وجود یا عدم وجود یک حالت اولیه که منجر به مقدار "درست" یا "۱" در جدول ارزش تابع گردد، مسئله ارضاپذیری نامیده می شود. در سال ۱۹۷۱، Cook نشان داد این مسئله یک مسئله NP– تمام است.	مسئلهٔ ارضاپذیری	satisfiability problem
یک حمله تعمیم یافته از حمله مربعی	حملهٔ اشباع	saturation attack
		s-box→substitution box
	مقیاس پذیر	scalable
پروتکلی بر مبنای RFC 1949، که در آن کلید در یک شبکه چند پخشی (Multicats) میان شرکت‌کنندگان توزیع می‌شود.	توزیعِ کلید چندپخشی مقیاس پذیر	scalable multicast key distribution (SMKD)
جستجو در دادهٔ باقیمانده بدون دارا بودن مجوز لازم، برای بدست آوردن داده‌های حساس.	زباله‌کاوی	scavenge
	طرح، شما	scheme
	طرحِ امضای اشنور	schnorr signature scheme
	درهم زن، درهم ریز	scrambler
نوعی حمله که در آن اطلاعات ارائه شده در صفحه نمایش مربوط به دارنده کارت اعتباری شنود می شود.	بریدن صفحه نمایش	screen scrapping
	گواهی‌نامه موقت	scrip
در برنامه‌نویسی رایانه‌ای به یک برنامه یا دنباله‌ای از دستورالعمل‌ها اطلاق می‌شود که یک منظور خاص را تأمین کرده و بتواند در داخل یک برنامه دیگر اجرا شود.	نبشته	script
یکی از ویژگی های توابع درهم ساز، که در صورت وجود این ویژگی با در اختیار داشتن m_1 ، یافتن m_2 به طوری که $hash(m_1) = hash(m_2)$، مشکل باشد.	مقاومت در برابر پیش تصویر دوّم	second preimage resistant= weak collision freeness
	راز	secret
همان سامانه رمز متقارن است که کلید بین دو طرف مشترک	سامانه رمز کلید مخفی	secret key cryptosystem

		و محرمانه است.
secret sharing scheme	طرح تسهیم راز، شمای تسهیم راز	
secure channel	کانال امن	
secure electronic transaction (SET)	تراکنش الکترونیکی امن	
secure socket layer (SSL)	لایهٔ دریچه امن	پروتکلی برای ایجاد ارتباط امن در اینترنت
security	امنیت	
security association (SA)	پیمان امنیتی	یک رابطه یک طرفه بین یک فرستنده و گیرنده است که خدمات امنیتی (نظیر رمزنگاری و احراز اصالت) را برای ارتباط بین فرستنده و گیرنده فراهم می‌کند.
security audit	ممیزی امنیتی	
security classification	طبقه‌بندی امنیتی	تعیین درجه خاص برای حفاظت از داده. مثل: سرّی، فوق سرّی و محرمانه
security evaluation	ارزیابی امنیتی	
security hole	رخنهٔ امنیتی	همان آسیب پذیری است، به vulnerability رجوع شود.
security identifier (SID)	شناسه امنیتی	
security incident	رخداد امنیتی	هشداری که نشان می‌دهد حمله‌ای رخ داده یا در حال رخ دادن است.
security label	برچسب امنیتی	برچسبی که حاوی اطلاعات نشان دهنده سطح امنیت یک سامانه است.
security policy	خط‌مشی امنیتی	
security violation	نقضِ امنیتی	
seed	بذر	داده‌هایی که به عنوان آغازگر یک رویه مورد استفاده قرار می‌گیرند.
selective forgery	جعل انتخابی	دسته‌ای از حملات علیه طرح‌های امضای دیجیتال
self synchronizing	خود همزمانی	
self-shrinking generator	مولد خود انقباضی	
self-signed certificate	گواهیِ خویش امضا	نوعی گواهی که توسط دارنده گواهی، امضا و به وسیله کلید عمومی مندرج در آن وارسی می‌شود.
self-synchronous	خودهمگام، خودهمزمان	
semantic security	امنیتِ معنایی	
semi-invasive attack	حمله شبه تجاوزی	در این حمله بر خلاف حمله تجاوزی، دستگاه رمزنگاری لزوماً از بسته‌بندی خارج نمی‌شود، اما با اتصال پروب‌های

		غیرمعمولی به تراشه، تلاش در جهت یافتن مقادیر داخلی آن انجام می‌شود. حمله تزریق خطا نمونه‌ای از یک حمله شبه تجاوزی است.
semi-weak key	کلیدِ نیمه ضعیف	
sensitive data	داده‌های حساس	
sensitive information	اطلاعات حساس	هر نوع اطلاعاتی که از دست رفتن، سوء استفاده، تغییر و یا دسترسی غیرمجاز به آنها بر منافع یک سازمان تأثیر نامطلوب داشته باشد.
sensitivity	حساسیت	معیاری جهت تعیین اهمیت اطلاعات، که توسط مالک اطلاعات به آنها نسبت داده می شود، تا سطح نیاز به حفاظت از آنها را مشخص کند.
separation of duties	تفکیک وظایف	عمل تقسیم مراحل کاری یک سامانه بین افراد مختلف با هدف جلوگیری از انحراف در اجرای عملیات آن توسط یک فرد خاص.
serial test	آزمونِ توالی	آزمونی آماری جهت بررسی میزان تصادفی بودن یک دنباله، در این آزمون تعداد الگوهای "۰۰"،"۰۱"،"۱۰"،"۱۱" در دنباله به صورت هم‌پوشان شمارش گردیده و با استفاده از توزیع مربع کای با درجه آزادی ۲، میزان تصادفی بودن دنباله تعیین می گردد.
Serpent		یکی از پنج الگوریتم رمز قالبی راه‌یافته به مرحله نهایی پروژه انتخاب AES .
server	کارگزار	
session hijacking	نشست ربایی	در طی ارتباط یک کاربر مجاز و یک کارگزار، نفوذگر ناگهان خود را به جای کاربر مجاز جا زده و ضمن ادامه نشست با کارگزار، مانع از ادامه ارتباط کاربر مجاز با کارگزار می گردد.
session key	کلیدِ جلسه، کلیدِ نشست	یک کلید موقت رمزنگاری بین طرفین ارتباط.
setup time	زمانِ برپایی	
setupc	برپایی، برپا کردن	
SHA (Secure Hash Algorithm)		مجموعه‌ای از توابع چکیده ساز که توسط NSA طراحی و منتشر گردید و توسط NIST به عنوان استاندارد توابع چکیده ساز معرفی گردید. سه ساختار متفاوت ارائه شده از این مجموعه SHA-0، SHA-1، SHA-2 نام دارند.
shadow	سایه	

shared key cryptosystem	سامانه رمزنگاری کلید مشترک	نام دیگری برای سامانه رمزنگاری متقارن.
shift register	ثبات انتقال	
short term	کوتاه مدت	
shrinking generator	مولد انقباضی	نوعی خاص از ساختارهای مبتنی بر انتقال نامنظم است که برای اولین بار در سال ۱۹۹۳ ارائه شد. در این ساختار از دو ثبات انتقال خطی یکی برای تولید دنباله خروجی و دیگری برای کنترل انتقال‌های ثبّات اول استفاده می‌شود.
side channel attack	حملهٔ کانال جانبی	نوعی حمله که بر اطلاعات حاصل از پیاده‌سازی الگوریتم رمز مبتنی است. این اطلاعات می‌تواند زمان اجرای الگوریتم، میزان توان مصرفی و یا تشعشعات الکترومغناطیسی سخت افزاری باشد که الگوریتم روی آن اجرا می‌شود.
sieving	غربال‌گری	
signatory	امضا کننده، صاحب امضا	
signature stripping	خلع امضا	
signcryption	امضارمز	فرآیندی مبتنی بر رمز کلید همگانی که هر دو عملکرد رمزنگاری و امضای دیجیتال را به طور همزمان فراهم می‌سازد.
significance level	سطح اهمیت	
simple network management protocol (SNMP)	پروتکل ساده مدیریت شبکه	پروتکلی برای مدیریت شبکه از راه دور، تا مدیر شبکه بتواند دستگاههای مختلف را زیر نظر داشته باشد یا حتی آنها را پیکربندی نماید.
simple power analysis (SPA)	تحلیلِ توانی ساده	به power analysis attack رجوع شود.
single-hop problem	مسئله یک جهشی	مخاطرات امنیتی ناشی از حرکت یک عامل نرم افزاری متحرک از سکوی خود به یک سکوی دیگر.
site	پایگاه	
slide key attack	حمله کلید لغزنده	باور غالب در طراحی رمزهای قالبی بر این است که افزایش تعداد دورهای الگوریتم موجب افزایش امنیت الگوریتم رمز و مقاومت بیشتر در برابر حملاتی مانند حمله تفاضلی است. حمله لغزنده با استفاده از نقاط ضعف موجود در ساختار تولید زیرکلیدها تلاش می‌کند اثر افزایش دورها را خنثی سازد.
smart card	کارت هوشمند	
smooth integer	عدد هموار	عدد صحیح مثبت n را y- هموار نامیم، هرگاه کلیه عوامل

اوّل آن کمتر یا مساوی y باشد.		
حمله‌ای از نوع منع خدمت است که از پروتکل ICMP استفاده می‌کند. در این حمله یک پیام جعلی ping با نام کارگزار هدف، برای آدرس‌های IP یک شبکه ارسال می‌شود که پاسخ‌های این پیام به آدرس کارگزار هدف برمی‌گردد و آن را از ارائه خدمت بازمی‌دارد.	حمله اِسمورف	Smurf attack
برنامه‌هایی برای جمع آوری و تحلیل داده های عبوری شبکه و احتمالا تشخیص مشکلات شبکه. سوء استفاده از این برنامه ها مبنای بسیاری از حملات است.	دیده‌بان	sniffer
جمع آوری و تحلیل ترافیک شبکه.	دیده‌بانی، به گوش ایستادن	sniffing
	نرم افزار گرا	software-oriented
	عاملِ حل پذیری	solving factor (SF)
	درستی	soundness
	مسیریابی منبع	source routing
		SPA→ simple power analysis
رایانامه‌های درخواست نشده، ناخواسته، نامربوط، ویا نامناسب، به ویژه نامه‌های تجاری و تبلیغاتی به تعداد زیاد.	هرزنامه	spam
	هرزنامه نگار	spammer
وقتی در یک دستگاه معادلات تعداد جملات ظاهر شده از حداکثر تعداد جملاتی که می‌توانست وجود داشته باشد، به طور قابل توجهی کمتر باشد، چنین دستگاه معادلاتی تُنُک نامیده می‌شود.	تُنُک	sparse
رویه‌ای برای کنترل و حفاظت چندگانه کلید، با تسهیم یا تقطیع کلید به مؤلفه‌ها. کلید ممکن است ابتدا تولید و سپس به مؤلفه‌هایی شکسته شود، یا ممکن است از ابتدا به صورت مؤلفه‌های مجزا تولید شود.	تقطیع دانش	split knowledge
اگر F یک میدان و f(x) یک چندجمله‌ای روی میدان F باشد، میدان K یک میدان تجزیه برای f(x) نامیده می شود، هرگاه: ۱) $F \subseteq K$ ۲) f(x) روی K به طور کامل تجزیه شود. ۳) K کوچکترین میدان توسیعی از F باشد که در شرایط (۱) و (۲) صدق می کند.	میدان تجزیه(گر)	splitting field
		SPN → Substitution Permutation Network

spoofed	جعلی	
spoofing	جعل هویت، جا زدن	یعنی خود را جای کس دیگری جا زدن.
spread spectrum transmission	انتقال طیف گسترده	
spy virus	ویروس جاسوس	
spyware	جاسوس افزار	
square attack	حمله مربعی	یک نوع حمله ساختاری.
SSL→Secure Socket Layer		
stage	طبقه، مرحله	
state	حالت	
state space	فضای حالت	
station to station key agreement protocol (STS)	پروتکل توافق کلید ایستگاه به ایستگاه	نسخه‌ای بهبود یافته از پروتکل دیفی- هلمن که در آن مشکل احراز اصالت حل شده است.
statistic	آماره	
statistical cryptanalysis	تحلیل آماری رمز	
status	وضعیت	
stealth virus	ویروس پنهان	نوعی ویروس که مخصوصاً برای پنهان ماندن از دید نرم افزارهای ضد ویروس طراحی شده است.
steganalysis	تحلیلِ نهان‌نگاری، نهان شکنی، نهان‌کاوی	تلاش برای تشخیص وجود یا عدم وجود پیام نهان شده در شیء پوششی.
steganography	نهان نگاری	در رمزنگاری هدف آن است که در صورت دسترسی دشمن به پیام، پیام در نظرش نامفهوم باشد و به مفهوم پیام دست نیابد. ولی در نهان نگاری هدف آن است که به طور کلی وجود پیام از نظر دشمن پنهان مانَد.
stego-object	نهان نگاشته	آنچه از ادغام داده های محرمانه در شئ پوششی(cover object) ایجاد می شود.
stop-and-go generator	مولد افت و خیز	
storage complexity	پیچیدگی ذخیره سازی	
stream cipher	رمزِ دنباله‌ای، رمزِ جریانی، رمزِ پی در پی	یک نوع رمز متقارن، در این رمز بیت‌های داده با عناصر یک دنباله شبه تصادفی ترکیب و متن رمزشده را تشکیل می‌دهند. دنباله شبه تصادفی معمولاً توسط ترکیبی از ثبات های انتقال با پس‌خورد خطی تولید می شود.
strength	استحکام	
strict avalanche criterion (SAC)	معیار بهمنی اکید	یک ویژگی از توابع بولی، هرگاه تغییر هر بیت ورودی یا

کلید، موجب تغییر کلیه بیت‌های خروجی با احتمال $\frac{1}{2}$ شود.		
یک نوع از حملات پویش درگاه.	حمله نورافکن چرخان	strobe
پیدا کردن زوج متمایز (x,y) به طوری که H(x)=H(y) از نظر محاسباتی ناممکن باشد.	مقاومت قوی در برابر برخورد	strong collision resistance
تابع چکیده‌سازی که علاوه بر خواص تابع چکیده‌ساز ضعیف، پیدا کردن یک زوج ورودی دلخواه که خروجی تابع به ازای آن دو یکسان باشد، از لحاظ محاسباتی غیر ممکن باشد.	تابع چکیده‌ساز قوی	strong hash function
	عدد اوّل قوی	strong prime
	عدد شبه اوّل قوی	strong pseudoprime
۱. حمله‌ای که در طراحی آن از ساختار ویژه رمز استفاده شده است، نظیر حمله مربعی در تحلیل AES. ۲. حملات یافتن کلید خصوصی از طریق کلید همگانی در سامانه رمزنگاری مَک اِلیس.	حمله ساختاری	structural attack
	حالت ناخواسته ساختاری	structural hazard
تابعی به صورت $e^{g(n)}$ که مرتبه $g(n)$ از n کوچکتر باشد، مثل $e^{\sqrt{n}}$	تابع زیرنمایی	subexponential function
	زیر روال	subroutine
	جانشینی	substitution
تابعی که در رمزهای متقارن به ویژه رمزهای قالبی جهت آشفته‌سازی به‌کار برده می‌شود. از خواص یک جعبه جانشینی خوب(مقاوم) آن است که هیچ رابطه خطی محتملی بین بیت‌های ورودی و بیت‌های خروجی آن وجود نداشته باشد، ضمناً هیچ تفاضلی در ورودی با احتمال خوبی به یک تفاضل مشخص در خروجی مربوط نشود. در رمزهای فایستلی لزومی ندارد که جعبه جانشینی معکوس پذیر باشد، ولی در رمزهای SPN، جعبه جانشینی حتماً باید معکوس پذیر باشد.	جعبه جانشینی	substitution box (s-box)
سامانه رمزی که در آن واحدهایی از متن اولیه طبق یک روال مشخص(دوطرفه) توسط واحدهایی از متن رمز جایگزین می‌شوند. این واحدها می توانند یک حرفی یا دو حرفی و یا حتی چند حرفی باشند. گیرنده با انجام عکس این	رمز جانشینی	substitution cipher

		عمل جایگزینی، متن رمز را رمزگشایی می‌کند.
substitution-permutation network	شبکه جانشینی- جایگشتی	
supersingular curve	منحنی ابرمنفرد	
surjective function	تابع پوشا	
swapping	تعویض، مبادله	
symbol	نماد	
symmetric cipher	رمزِ متقارن	سامانهٔ رمزی که کلید رمزنگاری و کلید رمزگشایی آن یکسان است.
symmetry	تقارن	
SYN flood attack	حملهٔ اشباع بسته SYN	یک نوع از حملات منع خدمت.
synchronous	همزمان، همگام	
T		
tag	برچسب	
tamper	دست‌کاری	عملی فیزیکی که حمله کننده عموماً بر روی سخت افزار رمزنگاری به منظور دستیابی و یا تغییر در مقایر میانی الگوریتم و با هدف کشف مقادیر مخفی (همچون کلید) انجام می‌دهد.
tamper resistant	مقاوم در برابر دست‌کاری	
tapping	انشعاب زنی	
TCP→ Transmission Control Protocol/Internet Protocol		
TCP→ Transmission Control Protocol/Internet Protocol		
TEMPEST		بررسی، مطالعه و کنترل برون تابی های افشاکننده‌ای که از تجهیزات مخابرات و سیستم‌های اطلاعاتی به صورت ناخواسته ساطع می‌شوند. (با وجود این‌که حروف این واژه بزرگ نوشته می‌شوند، این کلمه سَرنام نیست. هرچند ترکیب‌هایی بعداً پیشنهاد شده است که این واژه می تواند سَرنام آن‌ها نیز باشد.)
template attack	حمله الگویی	یکی از قوی‌ترین حملات تحلیل توانی و یا حملات تحلیل تشعشعات الکترومغناطیسی که با ساخت الگوهای سیگنال-های توان مصرفی و مقایسه آن‌ها با مقادیر اندازه‌گیری شده از دستگاه رمزنگاری سعی در کشف مقادیر مخفی آن دارد.

threat	تهدید	عامل بالقوه برای ایجاد یک حادثه نامطلوب برای امنیت سامانه.
threshold	آستانه	
threshold cryptography	رمزنگاری آستانه‌ای	نوعی رمز نامتقارن که در آن کلید رمزگشایی(خصوصی) بین چند نهاد تسهیم می‌گردد به گونه‌ای که عمل رمزگشائی تنها با مشارکت حداقل تعداد مشخصی از سهامدارن کلید خصوصی امکان پذیر باشد.
throughput	گذردهی	نرخ عبور داده از یک سامانه.
ticket	بلیط	
time memory data trade off (TMTO)	مصالحهٔ زمان- حافظه- داده	
time- memory trade-off attack	حملهٔ مصالحه زمان و حافظه، حملهٔ بده بستان زمان و حافظه	
time stamp	مُهرِ زمانی	اطلاعات زمانی درباره پیام که با آن گره می‌خورد.
timing attack	حملهٔ زمانی	یک نوع حمله کانال جانبی که دشمن با تحلیل زمان اجرای الگوریتم رمز سعی در یافتن بیت‌های کلید و یا اطلاعات مخفی دیگری دارد.
TM →Turing Machine		
TMTO→Time Memory Data Trade Off		
token	نشان	ابزار احراز اصالت، وسیله ای کوچک شبیه ماشین حساب جیبی یا کارت اعتباری جهت نگه‌داری مقدار کلید یا مقادیر مربوط به احراز اصالت و انجام محاسبات مربوط.
topology	توپولوژی	
total break	شکست کامل	دست‌یابی تحلیل‌گر به کلید.
trace	رد، اثر	
tracing	ردگیری، ردیابی	
tracking	رهگیری	
tractable	مهار شدنی	وقتی یک مسئله در یک زمان و فضای (حافظه) معقول قابل حل باشد.
trade-off	بده-بستان، مصالحه	
traffic analysis	تحلیل ترافیک	

transaction	تراکنش	
transaction authentication	احراز اصالت تراکنشی	
transparency	شفافیت	
transposition cipher	رمز جابه‌جایی	نوعی سیستم رمز که در آن جای حروف متن به هم می‌ریزد. البته این جابجایی جای حروف باید به گونه‌ای برگشت پذیر باشد تا انجام عمل رمزگشایی میسر باشد.
trapdoor function	تابع دریچه‌دار	تابعی که محاسبه آن آسان است، ولی محاسبه معکوس تابع بدون داشتن یک تعدادی اطلاعات اضافه بسیار سخت باشد، به این اطلاعات اضافه که محاسبه معکوس را برای دارنده آن بسیار راحت می‌کند، دریچه تابع گفته می‌شود.
trial and error	سعی و خطا	
triple A→AAA		
triple DES	DES سه‌گانه	یک نوع به‌کارگیری DES برای افزایش امنیت، در این روش ابتدا متن اصلی با یک کلید رمز شده و سپس با کلید دیگری رمزگشایی می‌شود. خروجی این مرحله با کلید اول مجدداً رمزگذاری می‌شود و متن رمز شده را تشککیل می-دهد. به طور خلاصه می توان این روش را به‌صورت $E_{k1}D_{k2}E_{k1}$ نمایش داد.
Trojan horse	اسب تراوا	یک برنامه کامپیوتری با تابعی به ظاهر و یا واقعاً مفید که به طور پنهانی دارای تعدادی توابع اضافی نیز هست که مخفیانه علیه سامانه عمل می‌کند.
truncated differentials attack	حمله تفاضلی بریده	تعمیمی از حمله تفاضلی علیه رمزهای قالبی که به جای استفاده از تفاضل کلی میان دو متن، از بخشی از آن استفاده می‌کند.
trust anchors	لنگرهای اعتماد	مجموعه‌ای از موسسات مورد اعتماد برای صدور گواهینامه.
trust chain	زنجیرهٔ اعتماد	
trust management (TM)	مدیریتِ اعتماد	
trusted third party(TTP)	شخص ثالث مُعتَمد	موجودیتی که ایجاد تعامل را برای دو طرفی که به او اعتماد دارند را تسهیل می کند. طرفین از این اعتماد، برای امن کردن تعاملاتشان استفاده می کنند.
trustee	مُعتَمد	
truth table	جدول درستی، جدول صحت	
tunneling	تونل‌زنی	ارسال بسته‌های اطلاعاتی از یک شبکه اختصاصی بر روی یک شبکه عمومی

Turing machine	ماشین تورینگ	ماشین محاسباتی فرضی با تعداد حالات محدود که دارای توان خواندن و نوشتن نامحدود است.
Twofish cipher	رمز Twofish	یک نوع الگوریتم رمز قالبی که برای پیاده‌سازی در پردازنده‌های توان پایین مثل کارت‌های هوشمند طراحی شده‌است.
U		
UDP scanning	پویش بسته‌های UDP	یک روش مخفیانه برای پی بردن به خدماتی که در یک میزبان دور در حال اجراست.
UDP tunneling	تونل زنی با بسته‌های UDP	ایجاد یک کانال مخفی ارسال داده‌ها در بسته‌های UDP که معمولاً برای ارسال داده استفاده نمی‌شوند. به این ترتیب امکان نشت اطلاعات بدون نظارت حفاظ و سامانه تشخیص نفوذ فراهم می‌شود.
unauthorized	غیرمجاز	
unblinding function	تابع بینا ساز	در مقابل blinding function
uncertainty	عدم قطعیت	
unconditional security	امنیت بدون شرط	
unforgeability	غیرقابل جعل بودن، جعل ناپذیری	
unicity distance	فاصلهٔ قابل شکست	حداقل طول متن رمز شده که با در اختیار بودن آن، سامانه رمز قابل شکست می شود.
unilateral authentication	احراز اصالت یک سویه	پروتکل احراز اصالتی که در آن فقط اصالت یکی از طرفین برای فرد مقابلش ثابت می شود.
unit	یگه، واحد	
universal forgery attack	حمله جعل فراگیر	
universal one-way hash function	تابع چکیده ساز یک طرفه فراگیر	همان تابع چکیده ساز ضعیف است.
unkeyed hash function	تابع چکیده ساز بدون کلید	
unlinkability	پیوند ناپذیری	
untraceablity	غیرقابل ردیابی	
urgent	فوری	
user account management	مدیریت حساب کاربران	شامل ۱) فرایند درخواست، ایجاد، صدور و لغو حساب‌های کاربران ۲) رهگیری کاربران و دسترسی‌های مجاز آن‌ها، و ۳) مدیریت عملکردهای فوق می‌باشد.
user ID	شناسه کاربر	

V		
validation	اعتبار سنجی	
verification	وارسی، راست آزمایی، درستی سنجی	
verification & validation (V&V)	درستی و اعتبار سنجی	
verifier	وارسی کننده، ارزیاب	
verify	وارسی کردن، ارزیابی کردن	
vernam cipher = one time pad cipher	رمز ورنام	
versatility	تنوع پذیری	
victim	قربانی	آن‌که مورد حمله قرار می‌گیرد.
virtual private network (VPN)	شبکه اختصاصی مجازی	شبکه‌ای اختصاصی که از یک شبکه عمومی (عموما" اینترنت)، برای ارتباط با سایت های راه دور و ارتباط کاربران بایکدیگر، استفاده می نماید.
virus	ویروس	یک قطعه برنامه که توانایی تکثیر خود را داشته و به برنامه دیگری الحاق می‌شود. در صورت آلوده شدن سیستم، مرتباً نسخه هایی از خود را تولید و به برنامه های دیگر الحاق می-کند.
virus hoax	بلوف ویروس	یک پیام هشدار فوری درباره ویروسی که واقعاً وجود ندارد.
visited network	شبکه میهمان	
visual cryptography	رمزنگاری بصری	
vote	رای	
vote submission facility (VSF)	تسهیلات رای‌گیری	
vulnerability	آسیب‌پذیری	نقض یا ضعف در طراحی، پیاده سازی، کارکرد یا مدیریت سامانه که می‌تواند برای نقض سیاست های امنیتی آن مورد سوء استفاده قرار گیرد.
vulnerability scanner	پویشگر نقاط آسیب پذیر	نرم افزارهایی که جهت شناسایی نقاط آسیب‌پذیر توسط نفوذگران مورد استفاده قرار می‌گیرند. این ابزارها به طور خودکار با فرآیند اجرا شده روی ماشین هدف ارتباط برقرار کرده و با ارسال داده‌های نا متعارف به آن فرآیند، نقطه ضعف آن را در مواجهه با این داده ها، بدست می‌آورند.
W		
warchalking	حمله شنود پیاده	شبیه wardriving، با این تفاوت که فرد پیاده به دنبال شنود امواج رادیویی است.

wardialing	حمله شماره‌گیری	اکتشاف تلفنی مودم‌ها، در این حمله نفوذگر از یک رایانه برای شماره‌گیری تعداد بسیاری شماره تلفن استفاده می‌کند تا سیستم‌های دارای مودم را شناسایی کند و پس از آن، بسته به این‌که چه برنامه‌ای به مودم پاسخ می‌دهد سعی می‌کند، رایانه او را تحت کنترل درآورد.
wardriving	حمله شنود سواره	عملیات جستجوی شبکه های بیسیم Wi-Fi توسط فردی در حال رانندگی در یک وسیله نقلیه با استفاده از یک رایانه قابل حمل و ابزار بی سیم.
warez	قفل شکسته	واژه‌ای که نفوذگران عموماً برای اشاره به نرم افزارهایی به کار می‌برند که به طور غیرقانونی، تکثیر و توزیع تجاری شده‌اند. این نرم افزارها اغلب حاوی ویروس‌ها، اسب‌های تروا و سایر کدهای بداندیش هستند و بنابراین دریافت و استفاده آنها بسیار مخاطره آمیز است.
warm site	پایگاه اطمینان بخش	یک فضای کاری با شرایط خاص محیطی که به میزان جزئی دارای تجهیزات IT و مخابرات است تا بتواند انجام عملیات IT را در یک مکان دیگر، در صورت رخداد یک تخریب عمده پشتیبانی نماید.
warrant	ضمانت	
watermarking	ته‌نقش نگاری، نشان گذاری	روشی برای حفظ حق مالکیت است که توسط آن شناسه‌ای از صاحب اثر در خود اثر به گونه‌ای تعبیه می‌شود که بدون ایجاد لطمه به کیفیت آن، به راحتی از آن قابل جداکردن نباشد و مشخص کننده منشاء و یا صاحب اثر باشد.
weak collision resistance	مقاومت ضعیف در برابر برخورد	به ازای هر x، پیدا کردن y به طوری که H(x)=H(y) از نظر محاسباتی مقدور نباشد.
weak hash function	تابع چکیده‌ساز ضعیف	
weak key	کلید ضعیف	کلیدی که در یک سامانه رمز، امنیت ضعیفی ایجاد کند. یعنی امنیت رمز به خاطر ساختار خاص کلید، کمتر از آن‌چه به طور معمول انتظار می رود، باشد.
web services	خدمات وب	نرم افزارهای کاربردی هستند که از طریق وب، قابل دسترسی بوده و مجموعه‌ای از عملکردها جهت انجام کسب و کار و یا هرگونه استفادهٔ دیگری را فراهم می‌آورند.
web site	پایگاه وِب	
web surfing	وب‌گردی	
wetware	مغز افزار	

white hat hacker	رخنه‌گر کلاه سفید	کسی که برای ارزیابی امنیت سیستم در برابر نفوذ، آن را مورد حملات آزمایشی قرار می‌دهد.
whitening	سفیدسازی	تکنیکی برای قدرتمندتر کردن رمزهای قالبی.
Wildcard Character	نویسهٔ عمومی	علامتی که می‌تواند به جای هر علامت دیگر و یا علامت‌های یک دنباله قرار داده شود. مانند آن‌چه به جای نام یک فایل نامعلوم در هنگام جستجوی فایل‌های داخل رایانه مورد استفاده قرار می‌گیرد و تمام فایل‌های با مشخصه مشترک را نشان می‌دهد.
wiretapping	جاسوسی، شنود خط	
withdrawn	برداشت	برداشت از حساب بانکی
witness	گواه، شاهد	
witness hiding protocol	پروتکل پنهان سازی گواه	
witness indistinguishability	تمایزناپذیری گواه	
word-oriented	کلمه‌گرا	
work factor	ضریب کار	حجم عملیات لازم برای کشف کلید.
workload	بارِکاری	
world wide web (www)	تارِ جهان گستر (وب)	
worm	کرم	نرم‌افزارهایی که خود را تکثیر می‌کنند و از طریق شبکه منتشر می‌شوند و بر خلاف ویروس‌ها برنامه‌های دیگر را آلوده نمی‌کنند.
wrapper	پوشش، لفافه	
X		
X.509		استانداردی برای صدور گواهینامه‌های دیجیتال که توسط ITU تایید شده است.
XOR→Exclusive OR		
XSS→Cross Site Scripting		
Z		
zero knowledge proof	اثبات هیچ آگاهی	
zero knowledge protocol	پروتکل هیچ‌آگاهی	یک پروتکل اثبات هیچ‌آگاهی، پروتکلی است که به وسیله آن یک عامل به نام اثبات کننده، اطلاع خود از یک راز را به یک عامل دیگر به نام وارسی کننده، به اثبات می‌رساند، به طوری که در خلال اجرای پروتکل، وارسی‌کننده هیچ گونه

آگاهی از راز پیدا نمی‌کند.		
روشی برای پاک کردن داده‌های ذخیره شده الکترونیکی، کلیدهای رمزنگاری و CSP ها با تغییر دادن یا حذف کردن محتویات داده‌های ذخیره‌شده، به منظور جلوگیری از بازیابی داده ها.	صفرسازی، نابود سازی	zeroization
		ZK protocl→Zero Knowledge protocol
به ماشین‌هایی که قربانی نفوذ بدخواهان شده‌اند و ناخودآگاه در حمله به یک سایت شرکت می‌کنند، اصطلاحا زامبی گفته می شود.	زامبی	zombie

فارسی به انگلیسی

الف

آرایه	Array
آزمون آماری فراگیر مارور	Maurer’s universal statistical test
آزمون اول بودن	primality test
آزمون پیچیدگی خطی	linear complexity test
آزمون تصادفی بودن	randomness test
آزمون توالی	serial test
آزمون ردیف	run test
آزمون زیبندگی	goodness of fit test
آزمون فراوانی	frequency test
آزمون نفوذپذیری	penetration test
آزمون نقطه عطف	change point test
آژانس امنیت ملی آمریکا	NSA(national security agency)
آستانه	Threshold
آسیب پذیری ها و رخنه‌پذیری‌های متداول	common vulnerabilities and exposures (CVE)
آسیب‌پذیری	vulnerability
آشغال گردی	dumpster diving
آشفتگی داده	data perturbation
آشفته ساز	confounder
آشفته سازی	Confusion
آگاهی	Awareness
آگاهی رسانی، پشتیبانی و امداد در حوادث رایانه ای	computer emergency response team (CERT)
آماره	Statistic
آمیختن، مخلوط سازی	mixing
آنتروپی	entropy
اَبر نمایی	hyperexponential

hyper link	اَبراتصال
hyper text	اَبرمتن
audit reduction tools	ابزار کاهش ممیزی
router audit tool(RAT)	ابزار ممیزی مسیریاب
anonymizers	ابزارهای گمنام ساز
key revocation	ابطال کلید، فسخ کلید
control connection	اتصال کنترلی
connection oriented	اتصال‌گرا
concurrent connection	اتصال هم‌روند
resource exhaustion	اتلاف منبع، هدر دادن منبع
prover	اثبات کننده
zero knowledge proof	اثبات هیچ آگاهی
avalanche effect	اثر بهمنی
fingerprint	اثرانگشت
effective	اثربخش، موثر
executive	اجرایی
authentication	احراز اصالت
electronic authentication (E-authentication)	احراز اصالت الکترونیکی
message authentication	احراز اصالت پیام
transaction authentication	احراز اصالت تراکنشی
deniable authentication	احراز اصالت حاشاپذیر
mutual authentication	احراز اصالت دوسویه/متقابل
challenge-response authentication	احراز اصالت مبتنی بر چالش و پاسخ
unilateral authentication	احراز اصالت یک سویه
authentication, authorization, and accounting (AAA)	احراز هویت، مجازشناسی، و حسابرسی
disruption	اختلال
jamming	اختلال
capture	اخذ

alarm	اخطار
crypto-anarchism	اخلال رمزنگاشتی
jammer	اخلال‌گر
merge	ادغام شدن
internet service provider (ISP)	ارائه کننده خدمات اینترنتی
inter host communication	ارتباط بین میزبان
inheritance	ارث‌بری
assess	ارزیابی
security evaluation	ارزیابی امنیتی
biased	اُریب
bias	اُریبی
Trojan horse	اسب تراوا
federal information processing standards(FIPS)	استانداردهای پردازش اطلاعات فدرال
public-key cryptography standards (PKCS):	استانداردهای رمزنگاری کلید همگانی
strength	استحکام
cryptographic strength	استحکام رمزنگاشتی
eavesdropping	استراق سمع، شنود
general deduction	استنباط کلی
deduction	استنتاج، قیاس
bug	اشکال
debug	اشکال زدایی
authenticity	اصالت، اعتبار
need to know principle = principle of least privilege	اصل دانستن در حد نیاز، اصل حداقل اجازه دسترسی
information	اطلاعات
sensitive information	اطلاعات حساس
certificate-related information	اطلاعات مرتبط با گواهی-نامه
validation	اعتبار سنجی
credentials	اعتبارنامه
pseudo-Mersenne primes	اعداد اول شبه مرسن

اعداد بلام	Blum integers
اعطای اعتبار نامه	accredit
اعلام دریافت	acknowledgment
افزونگی	redundancy
افشا	exposure
الزام	obligation
الگوریتم	algorithm
الگوریتم RSA	RSA algorithm
الگوریتم انتشار اطلاعات	information dispersal algorithm (IDA)
الگوریتم برلکمپ- مسی	Berlekamp–Massey algorithm
الگوریتم تصادفی	probabilistic algorithm
الگوریتم رمزگذاری A5/1	A5/1 encryption algorithm
الگوریتم قدم کوچک-قدم بزرگ	baby-step giant-step algorithm
امان سپاری	escrow
امان سپاری کلید	key escrow
امتیاز، حق انحصاری	patent
امضا کننده، صاحب امضا	signatory
امضارمز	signcryption
امضای الکترونیکی	electronic signature
امضای تایید کننده	designated confirmer signature = confirmer signature
امضای حمله، ردپای حمله	attack signature
امضای رقمی، امضای دیجیتال	digital signature
امضای کور	blind signature
امضای گروهی	group signature
امضای وکالتی	proxy signature
اَمن محاسباتی	computationally secure
امنیت	security
امنیت IP	IP security
امنیت ایده آل	ideal security

امنیت بدون شرط	unconditional security
امنیت پویا	proactive security
امنیت پیشرو	forward security
امنیت پیشرو کامل	perfect forward secrecy
امنیت تجربی	heuristic security
امنیت داده	data security
امنیت رایانه ای	computer security
امنیت سرتاسری	end to end security
امنیت سطح بندی شده	graduated security
امنیت شبکه	network security
امنیت قابل اثبات	provable security
امنیت قابل قبول	adequate security
امنیتِ مبنا	baseline security
امنیت مخابرات	communications security(COMSEC)
امنیت مشروط	conditional security
امنیت معنایی	semantic security
انباشتگر	accumulator
انتقال طیف گسترده	spread spectrum transmission
انتقال کلید	key transport
اندازهٔ موثر کلید	effective key size
انشعاب زنی	tapping
انصاف	fairness
انعطاف پذیری	flexibility
انقیاد	binding
انکار ناپذیری	non-repudiation
انکارپذیری باورکردنی	plausible deniability
انگشت نگاری از ICMP	ICMP fingerprinting
اولویت، حق تقدم	priority
ایجاد اتصال	connection setup / connection establishment
ایراد، اشکال	flaw
ایمن داشت	safeguard
ایمنی	safety

ایمنی از همبستگی	correlation immunity
اینترنت	internet

ب

بات	bot
بار	load
بار کاری	workload
بارکننده کلید	key loader
باز ارسال	forward(2)
بازرسی	inspection
بازیابی کلید	key recovery
بافر، حافظه میانی	buffer
باکتری	bacteria
بانک فروشنده	acquirer
بایگانی	archive
بَد نام	misnamed
بَدافزار	malware
بدون اتصال	connectionless
بدون برخورد	collision free
بدون رسید بودن	receipt-freeness
بده-بستان، مصالحه	trade-off
بَذر	seed
برخط	on-line
برپایی، برپا کردن	setupc
برچسب	tag
برچسب امنیتی	security label
برچسب شناسایی بسامد رادیوئی	radio frequency identification tag (RFID tag)
برخورد	collision
برداشت	withdrawn
بررسی جرایم رایانه ای	computer forensics
برقراری کلید، استقرار کلید	key establishment
برنامک	applet
برون تابی های مخاطره آمیز	compromising emanations

برون خط	off-line
بریدن صفحه نمایش	screen scrapping
بَسامد مشخصه (حروف)	characteristic frequency
بَستره توصیف اولویتهای حریم خصوصی	platform for privacy preference project(P3P)
بَستک	datagram
بَستک	packet
بسته	package
بلاتکلیف، معلق	pending
بلوتوث	Bluetooth
بلوف ویروس	virus hoax
بلیط	ticket
بمب منطقی	logic bomb
بودگاه	point of present (pop)
به مخاطره افتادن، تسخیرشدن، لو رفتن	compromise
بهبود پس از حمله، بازیابی پس از حمله	attack recovery
بی چَنگ	claw-free= claw-resistant
بی‌خبر	clueless
بی‌درنگ	real time
بیش‌تعریف	overdefined

پ

پارامتر امنیتی بحرانی	critical security parameter
پارسنگ، اقدام متقابل	countermeasure
پاس‌کاری	handoff
پاسخگویی	accountability
پاکسازی	purge
پاکسازی	sanitization
پاکت رقمی	digital envelope
پالایش محتوای کاربردی	application content filtering
پایانه فروش	point of sale (PoS)
پایش صفحه کلید	keystroke monitoring

پایش، نظارت	monitoring
پایگاه	site
پایگاه آماده‌باش	hot site
پایگاه اطمینان بخش	warm site
پایگاه خالی، پایگاه پوسته	cold site = shell site
پایگاه وب	web site
پایه، مبنا	base
پخش	broadcast
پراکُنش	diffusion
پرداخت خُرد	micro payment
پرداخت کلان	macro payment
پُرسمان	query
پُرسمان ممیزی	audit query
پرش فرکانسی	frequency hopping
پروتکل	protocol
پروتکل احراز اصالت کربروس	Kerberos authentication protocol
پروتکل انتقال پرونده	file transfer protocol(FTP)
پروتکل برش و انتخاب	cut-and-choose protocol
پروتکل پنهان سازی گواه	witness hiding protocol
پروتکل پیکربندی میزبان پویا	dynamic host configuration protocol (DHCP)
پروتکل تبادل (مبادله) کلید دیفی- هلمن	Diffie-Hellman key exchange = Diffie-Hellman key agreement = exponential key exchange
پروتکل تعهد	commitment protocol
پروتکل توافق کلید ایستگاه به ایستگاه	station to station key agreement protocol (STS)
پروتکل تولید کلید جلسه کنفرانس	conference keying protocol
پروتکل رمزگذاری دوگان	dual encryption protocol (DEP)
پروتکل ساده مدیریت	simple network management

شبکه	protocol (SNMP)
پروتکل شناسایی فیات شامیر	Fiat-Shamir identification protocol
پروتکل مدیریت کلید گروهی	group key management protocol (GKMP)
پروتکل واگشایی آدرس	address resolution protocol (ARP)
پروتکل همزمانی شبکه	network time protocol(NTP)
پروتکل هیچ آگاهی	zero knowledge protocol
پس‌رو	backward
پسخورد	feedback
پسماند داده ها	data remanence
پشتیبان	back up(n)
پشتیبان گرفتن	back up(v)
پُل	bridge
پنهان سازی	concealment
پنهان سازی	hiding
پنهان سازی اطلاعات	information hiding
پوچ	null
پوچ ساز	annihilator
پوشا	on-to
پوشانه، نقاب	mask
پوشش کلید، لفافه کلید	key wrap
پوشش گذاری، نقاب گذاری	masking
پوشش، لفافه	wrapper
پول الکترونیکی	electronic cash
پویا	dynamic
پویش بسته های UDP	UDP scanning
پویش درگاه	port scanning
پویشگر شبکه	network scanner
پویشگر نقاط آسیب پذیر	vulnerability scanner
پهنای باند	bandwidth
پیاده سازی	implementation

پیام چالش	challenge message
پیام ساختگی	dummy message
پیام کور	blinded message
پی‌جو	pager
پیچیدگی الگوریتم	algorithm complexity
پیچیدگی حافظه مجانبی	asymptotic space complexity
پیچیدگی خطی	linear complexity
پیچیدگی داده ها	data complexity
پیچیدگی ذخیره سازی	storage complexity
پیچیدگی زمان مجانبی	asymptotic time complexity
پیچیدگی محاسبات	computational complexity
پیش‌آگهی	precursor
پیش پرداخت	pre-paid payment
پیش پردازش	preprocess
پیشانه، پیشخوان	console
پیشرو	forward(1)
پیشکار	proxy server
پیشگو، سروش	oracle
پیشگوی تصادفی، سروش تصادفی	random oracle
پیکربندی	configuration
پیمان امنیتی	security association (SA)
پیمانه	module
پیمانه‌های قابل بارگذاری	loadable modules
پینگ	Ping (packet internet groper)
پیوست آلوده	infected attachment
پیوند ناپذیری	unlinkability
پیوند، یال	link

ت

تابع آشوبی	chaotic function
تابع برازندگی	fitness function
تابع بنت	bent function
تابع بینا ساز	unblinding function

surjective function	تابع پوشا
combining function	تابع ترکیب کننده
hash function	تابع چکیده ساز
collision free hash function	تابع چکیده ساز بدون برخورد
unkeyed hash function	تابع چکیده ساز بدون کلید
strong hash function	تابع چکیده ساز قوی
universal one-way hash function	تابع چکیده ساز یک طرفه فراگیر
weak hash function	تابع چکیده‌ساز ضعیف
trapdoor function	تابع دریچه‌دار
subexponential function	تابع زیرنمایی
almost perfect nonlinear function (APN)	تابع غیرخطی تقریباً کامل
compression function	تابع فشرده ساز
one-way function	تابع یک طرفه
impact	تأثیر
potential impact	تأثیر بالقوه
world wide web (www)	تار جهان گستر (وب)
freshness	تازگی
credentials service provider	تأمین‌کننده خدمات اعتبارنامه ها
confirmation	تایید
linear transformation	تبدیل خطی
data conversion	تبدیل داده ها
affine transformation	تبدیل مستوی
Hadamard transform	تبدیل هادامارد
adware	تبلیغ افزار
abstraction	تجرید
integer factorization	تجزیه به عوامل صحیح
atomicity	تجزیه ناپذیری
atomicity, consistency,	تجزیه ناپذیری، سازگاری،

عایقی، و ماندگاری	isolation and durability (ACID)
تجمیع، تجمع	aggregation
تحلیلِ آماری رمز	statistical cryptanalysis
تحلیلِ پیوند	link analysis
تحلیلِ تأثیر کسب و کار	business impact analysis (BIA)
تحلیلِ ترافیک	traffic analysis
تحلیلِ تفاضلی	differential cryptanalysis
تحلیلِ توانی ساده	simple power analysis (SPA)
تحلیلِ خطی	linear cryptanalysis (LC)
تحلیلِ خوشه‌ای	cluster analysis
تحلیلِ رمز، رمزشکنی	cryptanalysis
تحلیلِ نهان نگاری، نهان-کاوی	steganalysis
تحلیلِ یکپارچه	integral cryptanalysis
تحلیلگر رمز، رمزشکن	cryptanalyst
تخصیص	assignment
تخم مرغ عید	easter egg
تراشهٔ کلیپر	Clipper chip
تراکنش الکترونیکی امن	secure electronic transaction (SET)
تراکنش	transaction
ترتیب قاموسی	lexicographical order= dictionary order
ترجمهٔ نشانی شبکه	network address translate (NAT)
ترمیم	remediation
ترمیم داده	data restoration
تروریست(خرابکار) فضای تبادل اطلاعات	cyber terrorist
تسهیلات رای گیری	vote submission facility (VSF)
تسهیم اطلاعات	information sharing
تسهیم کننده، توزیع کننده	dealer
تشخیص سوءاستفاده	misuse detection
تشخیص ناهنجاری	anomaly detection

تشخیص نفوذ	intrusion detection
تصادفی	random
تصادفی بودن	randomness
تصفیه	filtering
تصفیه خروجی	egress filtering
تصفیه رایانامه	email filtering
تصفیه ورودی	ingress filtering
تضمین، اطمینان	assurance
تطابق	matching
تعامل	interaction
تعاملی	interactive
تعدیلِ بار، توازنِ بار	load balancing
تعمیم	generalization
تعویض، مبادله	swapping
تفکیک وظایف	separation of duties
تقارن	symmetry
تقاضای دسترسی	access request
تقریب مدار ترتیبی خطی	linear sequential circuit approximation (LSCA)
تقسیم وحل	divide and conquer
تقطیع دانش	split knowledge
تقلب رایانه ای	computer fraud
تک جمله‌ای	monomial
تک‌شمار	nonce
تکه تکه کردن، تقطیع	fragmentation
تکه، قطعه	fragment
تلهٔ ظرف عسل	honeypot
تمامیت داده، یکپارچگی داده	data integrity
تمایزگر	distinguisher
تمایزناپذیری	indistinguishability
تمایزناپذیری گواه	witness indistinguishability
تمرکز زدایی	decentralization
تناقض‌نمای روز تولد	birthday paradox

تُنُک	sparse
تنوع پذیری	versatility
توابع رجعت پذیر	resilient function
توازن	parity
توازن (ریاضی)، تعادل	balance
توافق کلید	key agreement
توپولوژی	topology
تورینه	mesh
توزیع کلید	key distribution
توزیع کلید چندپخشی مقیاس پذیر	scalable multicast key distribution (SMKD)
توزیع مجدد کلید	rekeying
توسیع کلید	key expansion
توکار	built-in
تولید زیر کلید	key schedule
تونل زنی با بسته های UDP	UDP tunneling
تونل‌زنی	tunneling
ته‌نقش نگاری شکننده	fragile watermark
تهدید	threat
ته‌نقش نگاری، نشان گذاری	watermarking

ث

ثبات انتقال	shift register
ثبات انتقال با پس‌خورد خطی	linear feedback shift register (LFSR)
ثبات انتقال با پس‌خورد غیرخطی	non-linear feedback shift register (NFSR)
ثبت خروج	Log off =Log out
ثبت رسمی کلید	key notarization
ثبت‌کننده صفحه کلید	key logger
ثبتِ ورود	Log on = Log in

ج

جاروب ICMP	ICMP sweep = ping sweep
جاسوس افزار	spyware

جاسوسی	espionage
جاسوسی، شنود خط	wiretapping
جانشینی	substitution
جانشینی تک الفبایی	monoalphabetic substitution
جانشینی چند الفبایی	polyalphabetic substitution
جایگشت	permutation
جدول توزیع تفاضلات	difference distribution table
جدول درستی، جدول صحت	truth table
جدول رنگین کمان	rainbow table
جدول مبنا	look up table
جرمِ رایانه ای	computer crime
جرم فضای تبادل اطلاعات	cybercrime
جریان داده	data stream
جستجوی فراگیر	exhaustive search
جعبه جانشینی	substitution box (s-box)
جعبه جانشینی فعال	active S-box
جعبه جایگشت	permutation box (P-Box)
جعل	fabrication
جعل	forgery
جعل DNS	DNS spoofing
جعل IP	IP spoofing
جعل انتخابی	selective forgery
جعل نشانی	address spoofing
جعل وجودی	existential forgery
جعلِ هویت، جا زدن	spoofing
جعلی	spoofed
جمع آزما، سرجمع	checksum
جنگِ اطلاعات	information warfare

چ

چارچوب	framework
چرخش	rotation
چرخه‌ای، دوری	cyclic

چکیدهٔ پیام	message digest
چکیده سازی داده‌ها	data compaction
چند به یک	many to one
چند به یک کردن	decimation
چند جمله‌ای مشخصه	characteristic polynomial
چند جمله‌ای معکوسه	reciprocal polynomial
چندالفبایی	poly alphabetic
چندامضایی	multisignature
چندجمله‌ای	polynomial
چندجمله‌ای اوّلیه	primitive polynomial
چندجمله‌ای تحویل ناپذیر	irreducible polynomial
چهارتایی	quartet

ح

حادثه	incident
حاضر بودن	liveness (principal liveness)
الحاق	attach
الحاق	concatenate
الحاقی	adjoint
حالت	state
حالت ناخواسته ساختاری	structural hazard
حداقل مجوز	least privilege
حریم خصوصی	privacy
حساب	account
حسابرسی	accounting
حساسیت	sensitivity
حفاظ پل	bridge firewall
حفاظ سطح کاربرد	application level firewall
حفاظ سطح مسیر	circuit level firewall
حفاظت	protection
حفاظت داده ها	data protection
حفاظت مرزی	boundary protection
حق نسخه‌برداری	copyright

حق واگذاری	copyleft
حق یا مجوز خروج	egress
حلقه	loop
حملات ICMP	ICMP attacks (Internet Control Message Protocol attacks)
حمله	attack
حمله ارزیابی کانال آشکار	clear channel assessment attack
حمله اِسمورف	Smurf attack
حمله اشباع	saturation attack
حمله اشباع بسته SYN	SYN flood attack
حمله اعمال تاخیر	forced delay attack
حمله افشاء	disclosure attack
حمله الگویی	template attack
حمله انسداد	clogging attak
حمله بازتاب	reflection attack
حمله براساس بردار اوّلیه منتخب	chosen IV attack
حمله بریدن و چسباندن	cut and paste attack
حمله بستاری	closure attack
حمله بومرنگ	boomerang attack
حمله به DNS	DNS attack
حمله پیش تصویر	preimage attack
حمله پیش-اجرا	pre-play attack
حمله تجاوزی	invasive attack
حمله تحلیل تشعشعات الکترومغناطیسی	electromagnetic analysis(EM) attack
حمله تحلیل توان	power analysis attack
حمله تحلیل توان تفاضلی	differential power analysis attack (DPA)
حمله تحلیل عیب	fault analysis attack
حمله تحلیل فراوانی حروف	frequency analysis attack
حمله تحلیل همبستگی توان	correlation power analysis attack (CPA)

حمله تصادفی	random attack
حمله تصحیح قالب	correcting block attack
حمله تفاضل ناممکن	impossible differential attack
حمله تفاضلی بریده	truncated differentials attack
حمله تقریب خطی	linear approximation attack
حمله تکرار	replay attack
حمله تمایز	distinguishing attack
حمله جبری	algebraic attack
حمله جستجوی پیشرو	forward search attack
حمله جستجوی فراگیر	brute force attack
حمله جستجوی فراگیر فضای کلید	exhaustive key search attack
حمله جعبه سیاه	black-box attack
حمله جعل	fabrication attack
حمله جعل فراگیر	universal forgery attack
حمله جعل کارگزار	host impersonation attack /server spoofing attack
حمله جعل هویت	Impersonation attack
حمله چاله خاکستری	gray hole attack
حمله چندوجهی	blended attack
حمله حدس وتعیین	guess and determine attack
حمله خصمانه	adversarial attack
حمله خوشه بندی کلید	key clustering attack
حمله داخلی	insider attack
حمله داده-مبنا	data-driven attack
حمله درج	insertion attack
حمله درون یابی	interpolation attack
حمله درهم بافی	interleaving attack
حمله دق الباب	doorknob rattling attack
حمله دو نقطه (..)	dot dot attack (..)
حمله روز تولد	birthday attack

حمله زمانی	timing attack
حمله زنجیره ای	chaining attack
حمله زنجیره ای نقطه ثابت	fixed-point chaining attack
حمله ساختاری	structural attack
حمله سازگاری خطی	linear consistency attack
حمله سرریز بافر	buffer overflow attack
حمله سیاه چاله	black hole attack
حمله سیلابی	flooding attack
حمله شبه تجاوزی	semi-invasive attack
حمله شماره گیری	wardialing
حمله شنود پیاده	warchalking
حمله شنود سواره	wardriving
حمله صیادی	phishing attack
حمله عام	generic attack
حمله غیرتجاوزی	non-invasive attack
حمله غیرفعال	passive attack
حمله فرد در میانه	man-in-the-middle attack(MITM)
حمله فعال	active attack
حمله فقدان در میانه	miss-in-the-middle attack
حمله فقط بر اساس کلید	key-only attack
حمله فقط براساس متن رمز	ciphertext only attack
حمله فیزیکی	physical attack
حمله کانال جانبی	side channel attack
حمله کاهش کیفیت خدمت	denial of quality of service (DoQoS)
حمله کتاب کد	codebook attack
حمله کدگشایی	decoding attack
حمله کلید لغزنده	slide key attack
حمله کلید مرتبط	related-key attack
حمله گریز	evasion attack
حمله مبتنی بر بردار اولیه معلوم	known IV attack
حمله مبتنی بر متن اصلی	known plaintext

معلوم	attack
حمله مبتنی بر واژه نامه	dictionary based attack
حمله متن اصلی منتخب	chosen plaintext attack
حمله متن اصلی منتخب وفقی	adaptive chosen plaintext attack
حمله متن رمز منتخب	chosen ciphertext attack
حمله متن رمز منتخب تمایز ناپذیر	indistinguishable chosen-ciphertext attack (IND-CCA)
حمله متن رمز منتخب وفقی	adaptive chosen ciphertext attack
حمله متن رمز منتخب وفقی تمایز ناپذیر	indistinguishable adaptive chosen-ciphertext attack (IND-CCA2)
حمله مربعی	square attack
حمله مستطیلی	rectangular attack
حمله مسیردهی غلط	misrouting attack
حمله مصالحه زمان و حافظه	time- memory trade-off attack
حمله ملاقات در میانه	meet in the middle attack
حمله منع احراز اصالت	denial of authentication attack
حمله منع خدمت	denial of service attack (DoS)
حمله منع سرویس توزیع‌شده	distributed denial of service(DDoS)
حمله میت‌نیک	Mitnick attack
حمله نقطه ثابت	fixed point attack
حمله نورافکن چرخان	strobe
حمله وارون سازی	inversion attack
حمله واژه نامه ای	dictionary attack
حمله همبستگی	correlation attack
حمله همرفت خطی	linear syndrome attack

خ

خاتمه اتصال	connection teardown
خاصیت همترازی	alignment property

خدمات وب	web services
خدمت راهنمایی متمرکز	centralized directory service
خط استیجاری	leased line
خط مشی	policy
خط مشی امنیتی	security policy
خط مشی امنیتی دیوار چین	chinese wall security policy
خط مشی دنیای بسته/باز	closed/open world policy
خطای با محل معین	erasure error
خطای قطاری	burst error
خط‌مشی گواهی	certification policy
خطی سازی	linearization
خطی سازی تکراری	relinearization
خلافکار (وب)	black webber
خلع امضا	signature stripping
خود وارون	involution
خود همبستگی	autocorrelation
خود همزمانی	self synchronizing
خود همگام، خود همزمان	self-synchronous
خودکاره	automaton
خودکاره حالت متناهی	finite state automaton
خودمختار	autonomous
خودمختاری	autonomy

د

دادگان، پایگاه داده ها	database
داده بان	data custodian
داده کاوی	data mining
داده‌های حساس	sensitive data
داده‌های طبقه بندی شده	classified data
داده‌های فعال سازی	activation data
داده‌های ممیزی	audit data
داده- همراه، داده-پیوست	associated data
داده، داده ها	data
دارایی	asset

دام‌گذاری	entrapment
دانش، دانایی	knowledge
دانه‌بندی	granularity
داور	arbiter
درِ پشتی	back door
درجه ایمنی جبری	algebraic immunity degree
درجه جبری	algebraic degree
درخت تصمیم گیری	decision tree
درخواست الحاق	join - request
درخواست امضای گواهی	certification sign request (CRS)
درخواست پژواک	echo request
درخواست مجوز	authorization request
درستی	soundness
درستی و اعتبار سنجی	verification & validation (V&V)
درگاه	port
درگاه داده	data port
دروازه	gateway
دروازه سطح مسیر	circuit level gateway
دروازه کاربرد	application gateway
دروازه، دریچه	gate
درون قلمرویی	inter realm
درون یابی	interpolation
درهم زن، درهم ریز	scrambler
دزدیده شده	captured
دست دادن	hand shaking
دستبرد	interception
دستداد	handshake
دسترس‌پذیری	accessibility
دسترسی، دستیابی	access
دست‌کاری	manipulation
دست‌کاری	tamper
دستیار رقمی شخصی	personal digital assistant (PDA)
دشمن	enemy

دشمن	opponent
دفتر ثبت رسمی	notary
دقت	precision
دکو	decoy
دلالت	implication
دنباله بیشینه	m-sequence = maximum length sequence
دنباله زدن، لایی گذاری	padding
دنبالهٔ کلید اجرایی	keystream
دو سویه	bijective
دودویی	binary
دور	round
دوگان	dual
دیده‌بان	sniffer
دیده‌بان بسته ها، شنودگر بسته‌ها	packet sniffer
دیده‌بانی، به گوش ایستادن	sniffing
دیوارِ آتش، حفاظ	firewall

ذ

ر

راز	secret
راز موقت	ephemeral secret
راهبری، اجرایی	administrative
رای	vote
رایانامه	email
رخ پوش، نقابدار	masquerader
رخ پوشی، نقاب گذاری	masquerading
رخ‌داد امنیتی	security incident
رخنه	breach
رخنه افزار	rootkit
رخنه امنیتی	security hole
رخنه کردن، نفوذ کردن	hack
رخنه‌گر کلاه خاکستری	grey hat hacker
رخنه‌گر کلاه سفید	white hat hacker

رخنه‌گر،نفوذگر	hacker
رخنه‌گری، نفوذگری	hacking
ردّ دسترسی	access denied
رد، اثر	trace
ردگیری، ردیابی	tracing
رده	class
رده بند	classifier
رده بندی	classification
رده پیچیدگی BPP	BPP complexity class
ردهٔ مجرد	abstract class
ردیف	run (of a sequence)
رسمی سازی	notarization
رقمی، دیجیتال	digital
رلهٔ کاربرد	application relay
رمز	cipher
رمز Twofish	Twofish cipher
رمز با کلید یکبار مصرف	one-time-pad cipher
رمز پِلِیفر	Playfair cipher
رمزِ پیشرو	forward cipher
رمزِ ترکیبی، رمز ضربی	product cipher
رمزِ تصادفی	probabilistic encryption
رمزِ جابه‌جایی	transposition cipher
رمزِ جانشینی	substitution cipher
رمزِ خودکلید	auto-key cipher
رمزِ دنباله‌ای جمع شونده	additive stream cipher
رمزِ دنباله‌ای، رمز جریانی	stream cipher
رمزدوره	cryptoperiod
رمزِ سزار	Caesar cipher
رمز شده	enciphered
رمز شده	encrypted
رمزشکن	code breaker
رمز قالبی	block cipher
رمز کاملیا	Camellia cipher

رمز کلید همگانی	public key cipher
رمزِ کلید همگانی احتمالاتی	probabilistic public-key encryption
رمزگذاری	encipher
رمزِ متقارن	symmetric cipher
رمز متوالی	cascade cipher
رمزِ مخلوط ساز	mixing cipher
رمزِ نامتقارن	asymmetric cipher
رمزِ ورنام	vernam cipher
رمزآوا	ciphony
رمزساز	code maker
رمزشناختی	cryptological
رمزشناس	cryptologist
رمزشناسی	cryptology
رمزگذاری	encrypt
رمزگذاری	encryption
رمزگذاری پخش	broadcast encryption
رمزگذاری ترکیبی	hybrid encryption
رمزگذاری توام با احراز اصالت	authenticated encryption (AE)
رمزگذاری چندگانه	multiple encryption
رمزگذاری حاشاپذیر	deniable encryption
رمزگذاری داده‌ها	data encryption
رمزگذاری دوگانه	double encryption
رمزگذاری سرتاسری	end to end encryption
رمزگذاری قطعی	deterministic encryption
رمزگذاری کلید همگانی الجمال	ElGamal public-key encryption
رمزگذاری کلید همگانی رابین	Rabin public-key encryption
رمزگذاریِ همه یا هیچ	all-or-nothing encryption
رمزگشایی	decryption
رمزگشایی داده‌ها	data deciphering

رمزگشایی داده‌ها	data decryption
رمزگشایی کردن	decipher
رمزگشایی کردن	decrypt
رمزنگار	cryptographer
رمزنگاری	cryptography
رمزنگاری آستانه ای	threshold cryptography
رمزنگاری بصری	visual cryptography
رمزنگاری سبک	lightweight cryptography
رمزنگاری کوانتومی	quantum cryptography
رمزنگاری مالی	financial cryptography (FC)
رمزنگاری مبتنی بر خم بیضوی	elliptic curve cryptography
رمزنگاشت	cryptogram
رمزنگاشتی	cryptographic
رمزهای سنتی	classic ciphers
روش p-1 پلارد	Pollard p-1 method
روش ارزیابی	assessment method
روش روِ پلارد	Pollard Rho method
رونوشتِ محرمانه (ر.ن.م)	blind carbon copy (BCC)
رویداد	event
رویدادگرا	event oriented
رویدادنگار	event logger
رویدادنگار، رخداد نما	log
رویدادنگاری، رخدادنگاری	logging
رویه	procedure
رویه ارزیابی	assessment procedure
رهگیری	tracking
ریسک، مخاطره	risk

ز

زامبی	zombie

زباله کاوی	scavenge
زبان توصیف خط مشی	policy description language (PDL)
زبان توصیف معماری	architecture description language(ADL)
زبان نشانه گذاری ابرمتنی (زنگام)	hypertext markup language (HTML)
زمان اجرا	run time
زمان انقضا	expiry time
زمان برپایی	setup time
زمان چندجمله ای	polynomial time
زمان ماموریت	mission time
زنجیره	chain
زنجیره اعتماد	trust chain
زنجیره حفاظت	chain of custody
زوج کلید	key pair
زوج هم‌گواه	cross certificate pair
زیر روال	subroutine
زیر ساخت کلید همگانی	public key Infrastructure (PKI)
زیردنباله ورچین شده	decimated subsequence
زیرساخت	infrastructure
زیست سنجشی	biometrics(2)
زیست سنجه	biometrics(1)

س

سابقهٔ ممیزی، ثبت ممیزی	audit record
ساختار فَیستلی	Feistel construction
ساختار مرکل دمگارد	Merkle-Damgard construction
سازگاری	compatibility
سازگاری حافظه‌ی نهان	cache consistency
ساز وکار	mechanism
سامانهٔ اطلاعات	information system
سامانهٔ پُرتأثیر	high impact system
سامانه پشتیبانی	backup system
سامانه تشخیص نفوذ	intrusion detection system (IDS)

سامانه تشخیص نفوذ شبکه مبنا	network IDS base
سامانه تعبیه شده	embedded system
سامانه رمز	cryptosystem
سامانه رمز کلید مخفی	secret key cryptosystem
سامانه رمز مک اِلیس	McEliece cryptosystem
سامانه رمزنگاری کلید خصوصی	private key cryptosystem
سامانه رمزنگاری کلید مشترک	shared key cryptosystem
سامانه رمزنگاری متعارف	conventional cryptosystem
سامانه فایل‌های شبکه	network file system (NFS)
سامانه کاملا امن	perfectly secure system
سامانه کم تأثیر	low impact system
سامانه نام دامنه	domain name system (DNS)
سایه	shadow
سَبک	mode
سَبک به‌کارگیری، سبک اجرایی	operating mode
سَبک پس‌خورد خروجی	output feedback mode(OFB)
سَبک پس‌خورد رمز	cipher feedback mode(CFB)
سَبک زنجیره‌ای قالبهای رمز	cipher block chaining mode(CBC)
سَبک شمارنده	counter mode= integer counter mode, segmented integer counter mode
سَبک شمارنده	integer counter mode(ICM)= Counter mode
سَبک کتابچه رمز	electronic codebook operating mode (ECB)
سخت افزار- گرا	hardware-oriented
سرریز	over flow

سرآیند	header
سرآیند احراز اصالت	authentication header (AH)
سراسری	global
سربار	overhead
سرتاسر، انتها به انتها	end to end
سرریز بافر	buffer overflow
سرقت کلیک	clickjacking
سرقت نگاری	kleptography
سرقت، ربودن	hijacking
سَرنام	acronym
سطح اهمیت	level of significance
سطح اهمیت	significance level
سطح بحران	criticality level
سعی و خطا	trial and error
سفت افزار	firmware
سفید سازی	whitening
سفید کردن کلید	key whitening
سکه الکترونیکی	electronic coin
سلسله ممیزی	audit trail
سند	document
سوء استفاده	abuse
سوءاستفاده فعال	active misuse
سیاه چاله	black hole
سیاه کلاه	black hat
سیستم رمز منصف	fair cryptosystem
سیل نامه، توده نامه	mass mail (MM)
سیلاب سازی	flooding
سیلاب سازی ICMP	ICMP flood

ش

شاه‌کلید، کلید اصلی	master key
شبکه	network
شبکه آمیزنده	mix net
شبکه اختصاصی مجازی	virtual private network (VPN)
شبکه اقتضایی	Ad hoc network

شبکه بات	botnet
شبکه بافی	network weaving
شبکهٔ تله عسل	honeynet
شبکهٔ جانشینی-جایگشتی	substitution-permutation network
شبکهٔ خصوصی	private network
شبکهٔ داخلی، شبکه محلی	local area network (LAN)
شبکهٔ شخصی	personal area network (PAN)
شبکهٔ میهمان	visited network
شبکهٔ شهری	metropolitan area network
شبکهٔ محلی	local area network (LAN)
شبه اوّل	pseudoprime
شبه برخورد	pseudo collision
شبه تصادفی	pseudorandom
شبه حمله	pseudo attack
شخص ثالث مُعتَمَد	trusted third party(TTP)
شفافیت	transparency
شکاف دنباله	gap of a sequence
شکست کامل	total break
شکست نظری	academic break
شکستن	break
شکل پذیری	malleability
شکل ناپذیر	non-malleable
شماره شناسایی شخصی	personal identification number (PIN)
شمای امضای احتمالاتی	probabilistic signature scheme (PSS)
شناسایی، تعیین هویت	identification
شناسه	identity
شناسه امنیتی	security identifier (SID)
شناسه تمایز	distinguishing identifier
شناسه رقمی/ دیجیتال	digital ID
شناسهٔ کاربر	user ID

شیئ پوششی	cover object

ص

صاحب کارت	cardholder
صادرکننده کارت	card issuer
صافی محتوا	content filter
صدور گواهی و اعطای اعتبار	certification and accreditation (C&A)
صدورِ مجوز، مجاز شناسی	authorization
صفرسازی، نابود سازی	zeroization
صورتِ نرمال جبری	algebraic normal form(ANF)
صوری	formal

ض

ضد ویروس	antivirus
ضریب کار	work factor
ضمانت	warrant
ضمنی	implicit

ط

طبقه بندی امنیتی	security classification
طبقه، مرحله	stage
طرح امضای اشنور	schnorr signature scheme
طرح امضای الجمال	ElGamal signature scheme
طرح بازیابی پس از سانحه	disaster recovery plan (DRP)
طرح بازیابی کسب و کار	business recovery-rsumption plan (BRP)
طرح تداوم کسب و کار	business continuity plan (BCP)
طرح تسهیم راز	secret sharing scheme
طرح رخداد پذیر	contingency plan
طرح رمزگذاری نیدِرِیتر	Niederreiter encryption scheme
طرح، شما	scheme
طرد	discard
طرف ارتباط	principal
طول قالب، اندازه قالب	block length=block size

طول، مدت	duration
طولانی مدت	long term

ع

عامل	agent
عامل حل پذیری	solving factor (SF)
عامل مبنا	agent based
عبارت عبور	passphrase
عددِ انشعاب	branch number
عدد اوّل ایمن	safe prime
عدد اوّل قوی	strong prime
عدد شبه اوّل قوی	strong pseudoprime
عدد مرسن	Mersenne number
عدد هموار	smooth integer
عدم اجبار	coercion resistance
عدم اجبار	incoercibility
عدم قطعیت	uncertainty
علامت، نشانه	badge
عمر، طول عمر	life time
عمل	action
عملوند	operand
عیب	fault
عیب یابی	fault detection

غ

غربال میدان اعداد عام	general number field sieve
غربالگری	sieving
غلبه داشتن	dominate
غیر تعاملی	non-interactive
غیر خطی بودن	nonlinearity
غیرقابل جعل بودن	unforgeability
غیرقابل ردیابی	untraceablity
غیرمجاز	unauthorized
غیرمخرب	non-malicious

ف

فاصله قابل شکست	unicity distance

فاصله ویرایشی	edit distance
فاصله همینگ	hamming distance
فراداده	meta data
فراوانی حرف	letter frequency
فرایند	process
فرض کرشهف	Kerckhoffs' assumption
فشرده سازی داده‌ها	data compression
فضای تبادل اطلاعات	cyberspace
فضای حالت	state space
فضای کلید	keyspace
فقدان	miss
فناوری اطلاعات (فا)	information technology (IT)
فوری	urgent
فهرست بررسی	check list
فهرست راهنمای همگانی	public directory
فهرست سیاه	blacklist
فهرست کنترل دسترسی	access control list (ACL)
فهرست گواهی‌های باطل‌شده (فسخ شده)	certificate revocation list (CRL)

ق

قاب	frame
قابل شکست	breakable
قابلیت اطمینان	reliability
قابلیت دسترسی	availability
قابلیت ممیزی	auditability
قابلیت همکاری	interoperability
قالب	block (1)
قالب محتوا	content format
قانونی	legitimate
قبول	accept
قرارداد	contract
قربانی	victim
قضیه باقیمانده چینی	chinese remainder theorem (CRT)

قضیه بیز	bayes’ theorem
قطع	abort
قطع اتصال	disconnection
قطع ارتباط	outage
قطعی، یقینی	deterministic
قفل شکسته	cracked
قفل شکسته	warez
قفل شکن	cracker
قفل شکنی	cracking
قلاب	hook
قلمرو، ناحیه	realm
قید	constraint

ک

کارآیی	efficiency
کاربر خاطی	misfeasor
کاربرد	application
کارت اعتباری	credit card
کارت پیش پرداخت	debit card
کارت هوشمند	smart card
کارخواه، مشتری	client
کارگزار	server
کانال امن	secure channel
کانال پنهان	covert channel
کاه دادن و باد دادن	chaffing and winnowing
کتاب کد	codebook
کُد	code
کُد BCH	BCH code
کُد MDS	MDS code
کُد احراز اصالت پیام	message authentication code (MAC)
کُد تشخیص تغییر	modification detection code (MDC)
کُد تشخیص خطا	error detection code
کُد تشخیص دست‌کاری	manipulation detection code

کُد تصحیح خطا	error correction code
کُد دوری	cyclic code
کُد سخت	hard-code
کُد سوء استفاده	exploit code
کُد عملگر	Opcode (operand code)
کُد گوپا	Goppa code
کُد یکپارچگی پیام، کُد تمامیت پیام	message integrity code (MIC)
کُدگذار	encoder
کُدگذاری	coding
کُدگذاری	encode
کُدگشا	decoder
کُدگشایی کردن	decode
کران	bound
کِرم	worm
کلمه عبور، گذر واژه	password
کلوچک	cookie
کلید	key
کلید اجرایی	running key
کلید از پیش مشترک	preshared key
کلید اوّلیه	primary key
کلید برگرفته	derived key
کلیدِ جلسه، کلید نشست	session key
کلیدِ خصوصی	private key
کلیدِ دور	round key
کلیدِ ضعیف	weak key
کلیدِ عبور	passkey
کلیدِ مرتبط	related key
کلیدِ موقت	ephemeral key
کلیدِ نیمه ضعیف	semi-weak key
کلیدِ همگانی	public key
کنارگذر	bypass
کنترل پیکربندی	configuration control
کنترل دسترسی	access control

کنترل دسترسی اختیاری	discretionary access control
کوتاه مدت	short term
کورسازی	blinding
کیف پول الکترونیکی	electronic wallet
کارایی	performance
کاربر نهایی	end user
کارگزار احراز اصالت	authentication server (AS)
کارگزار دسترسی	access server
کارگزار دسترسی شبکه	network access server (NAS)
کُد شناسه	ID Code
کُد عروسک	doll code
کلمه‌گرا	word-oriented

گ

گذر کُد، کُد عبور	passcode
گذردهی	throughput
گذرواژه یکبارمصرف	one-time password
گرداننده	handler
گروه دوری	cyclic group
گره	node
گسترش چندمنظوره رایانامه	MIME(Multipurpose Internet Mail Extension)
گلوگاه	bottleneck
گمنام، ناشناس	anonymous
گمنامی، ناشناسی	anonymity
گواه دیجیتالی/رقمی	digital evidence
گواه، شاهد	witness
گواهی	certification
گواهی اوّل بودن	certificate of primality (or primality certificate)
گواهی خویش امضا	self-signed certificate
گواهی متقابل	cross certification
گواهی نامعتبر	bad certificate

گواهینامه	certificate
گواهینامه دو منظوره	dual-use certificate
گواهینامه رقمی/دیجیتال	digital certificate
گواهینامه موقت	scrip
گوفر	gopher

ل

لایه	layer
لایه پیوند داده‌ها	data link layer
لایه دریچه امن	secure socket layer (SSL)
لایه کاربرد	application layer
لایی گذاری بهینه رمز نامتقارن	Optimal Asymmetric Encryption Padding (OAEP)
لرزه	jitter
لغو کردن	abrogate
لفافه‌بندی	encapsulation
لنگرهای اعتماد	trust anchors

م

مازه، ستون فقرات	backbone
ماشین تورینگ	Turing machine
ماشین حالت متناهی	finite-state machine
مامور امنیت سامانه اطلاعات	information system security officer (ISSO)
ماموریت پذیری	missionability
ماندگار	persistent
مبادله الکترونیکی داده	electronic data interchange
مبادلهٔ کلید	key exchange
مبتنی بر بیت، بیت‌گرا	bit-oriented
مبتنی بر رویداد، رویداد مبنا	event driven
مبتنی بر میزبان	host-based
مبنا گذاری	baselining
متباین، نسبت به هم اول	coprime
متخاصم، خصم	adversary
متن اصلی	cleartext = plaintext

متن اصلی	plaintext
متن رمز شده، متن رمز	ciphertext
متناوب	alternating
متوازن (ریاضی)، متعادل	balanced
مثال نقض	counterexample
مثبت غلط	false positive
مجاز	authorized
مجاز بودن	eligibility
مجاز شناس دسترسی	access authority
مجازشناس ویژگی	attribute authority
مجموعه قوانین حفاظ	firewall ruleset
مجوز ثبت محلی	local registration authority (LRA)
محاسبات توزیع‌شده	distributed computing
محافظ با اطمینان بالا	high assurance guard (HAG)
محافظ(سامانه محافظ)	guard (system guard)
محتوای فعال	active content
محدودیت دسترسی	access restriction
محرمانگی	confidentiality
محرمانگی پیشرو	forward secrecy
محیط حفاظ	firewall environment
محیط محاسباتی گسترده	pervasive computing environment
مخاطره مرتبط با IT	IT-related risk
مخزن	repository
مخفی سازی پیام	message concealing
مدخل، درایه	entry
مدرک دیجیتال نسخه دوّم	duplicate digital evidence
مدعی	claimant
مدل احتمالاتی	probabilistic model
مدل کارخواه/کارگزار	client/server model
مدل‌سازی تحلیلی	analytic modeling
مدیریت اعتماد	trust management (TM)

مدیریت حساب کاربران	user account management
مدیریت کلید	key management
مراقبت الزامی	due care
مراکز مجاز منطقه ای	regional authority (RA)
مربع لاتین	latin square
مرتبه رجعت پذیری	resiliency order
مرتبه، درجه	order
مرجع صدور گواهی	certification authority (CA)
مرجع مجاز شناس	authority
مرحله پردازش اتصال	connection handling stage
مرکز اطلاعات شبکه	network information center (NIC)
مرکز ترجمه کلید	key translation center (KTC)
مرکز صدور گواهی ریشه	root CA
مرکز توزیع کلید	key distribution Center(KDC)
مرورگر	browser
مسئله ارضاپذیری	satisfiability problem
مسئله سخت	hard problem
مسئله سرکش	intractable problem = hard problem
مسئله کوله پشتی	knapsack problem
مسئله لگاریتم گسسته	discrete logarithm problem
مسئله نزدیک ترین بردار	closest vector problem(CVP)
مسئله یک جهشی	single-hop problem
مسئولیت فضای تبادل اطلاعات	cyber liability
مسائل از درجه سختی فراتر از چندجمله ای	NP Problems
مسائل از نوع چند جمله ای	p-problems
مساله نمایش	representation problem
مستحکم سازی	hardening

مسدود کردن	block (2)
مسموم کردن DNS	DNS cache poisoning
مسیریاب تصفیه	filtering router
مسیریابی غیردقیق منبع	loose source routing
مسیریابی منبع	source routing
مشبّکه	lattice
مشخصه	characteristic
مصالحه زمان–حافظه–داده	time memory data trade off (TMTO)
مصوب	approved
مطمئن	reliable
معادله دیوفانتین	Diophantine equation
معتبر شناختن	accreditation
معتَمَد	trustee
معناشناسی محض	mere semantics
معیار ارزیابی	evaluation metric
معیار استقلال بیتی	bit independent criterion (BIC)
معیار انتشار	propagation criterion
معیار بهمنی اکید	strict avalanche criterion (SAC)
معیار ناهمواری	measure of roughness
مغزافزار	wetware
مقاوم بودن	robustness
مقاوم در برابر دست‌کاری	tamper resistant
مقاوم سازی مرکل–دمگارد	Merkle-Damgard strengthening
مقاومت در برابر برخورد	collision resistance
مقاومت در برابر پیش تصویر	preimage resistance
مقاومت در برابر پیش تصویر دوّم	second preimage resistant weak
مقاومت ضعیف در برابر برخورد	weak collision resistance

مقاومت قوی در برابر برخورد	strong collision resistance
مقدار اوّلیه	initial value (IV)
مقدار بررسی تمامیت، معیار تمامیت	integrity check value (ICV)
مقداردهی اوّلیه	initialization
مقدمه	preamble
مقیاس پذیر	scalable
مکرر، تکراری	iterated
ممانعت از نسخه برداری	copy protection
ممیزی	audit
ممیزی امنیتی	security audit
منحنی اَبرمنفرد	supersingular curve
منطق BAN	BAN logic
منطق توصیفی	description logic
منطق ممیزی	audit logic
منطقهٔ بی‌طرف، منطقهٔ حائل	demilitarized zone (DMZ)
منع، ممانعت، انکار، حاشا	deny
منفی غلط	false negative
مواد تولید کلید	key generation material
موسسه ملی استاندارد و فناوری	national institute of standard and technology(NIST)
مولد	generator
مولد اعداد تصادفی	random number generator
مولد اعداد شبه تصادفی	pseudo-random number generator (PRNG)
مولد افت و خیز	stop-and-go generator
مولد انقباضی	shrinking generator
مولد با فرمان ساعت	clock-controlled generator
مولد با گام متغیر	alternative step generator
مولد بلام–بلام–شاب	Blum–Blum–Shub generator
مولد خود انقباضی	self-shrinking generator

مولفه	component
مهاجم	attacker
مهار شدنی	tractable
مُهرِ زمانی	time stamp
مهر و موم داده ها	data seal
میان گذاری، درهم بافی	interleaving
میدان	field
میدان تجزیه(گر)	splitting field
میدان متناهی	finite field
میزبان به شبکه‌ی‌محلی	host to LAN
میزبان سنگر	bastion host
میزبان-به-میزبان	host to host
میلیون دستورالعمل در ثانیه	million instrument per second (MIPS)

ن

نا امنی	insecurity
ناچیز	negligible
ناف	hub
نام مستعار	alias
نام مستعار	pseudonym
نامانداگار	nonpersistent
نامه پراکن	remailer
نامه دان	mailbox
ناوش، ناوبری	navigation
ناهم‌زمان	asynchronous
نبشته	script
نبشته سایت قلابی	cross site scripting(XSS)
نرخ پذیرش غلط	false acceptance rate
نرم افزار گرا	software-oriented
نرم افزار مخرب	malicious software
نشان	token
نشان احراز اصالت	authentication token
نشان رمزنگاشتی	cryptographic token
نشانی	address

نشت اطلاعات	information leakage
نشست ربایی	session hijacking
نظریه پیچیدگی	complexity theory
نظریه پیچیدگی محاسبات	computational complexity theory
نظیر به نظیر، همتا به همتا	peer to peer
نفوذ	intrusion
نفوذ	penetration
نفوذگر	intruder
نقاب شبکه	net-mask
نقض امنیتی	security violation
نگاشت	mapping
نگهبان	bouncer (BNC)
نگهداری	maintenance
نگهداری اتصال	connection maintenance
نماد	symbol
نماد *O* بزرگ	big-*O* notation
نماینده کنترل حفاظ	firewall control proxy
نماینده کاربرد	application proxy
نمایه	profile
نمک زنی	salting
نمک، چاشنی	salt
نمودار ستونی	histogram
نمودار فعالیت	activity diagram
نوفه، اغتشاش	noise
نویسه	character
نویسهٔ عمومی	Wildcard Character
نهان سازی	caching
نهان‌سازی چند سطحی	multilevel caching
نهان‌نگاری	steganography
نهان‌نگاری زبان شناختی	linguistic steganography
نهان‌نگاشته	stego-object

و

verify	وارسی کردن، ارزیابی کردن
verifier	وارسی‌کننده، ارزیاب
verification	وارسی، راست آزمایی، درستی‌سنجی
invertible	وارون‌پذیر
interface	واسط
application programming interface (API)	واسط برنامه نویسی کاربردی
network interface	واسط شبکه
reactive	واکنشی
web surfing	وب‌گردی
access control entry (ACE)	ورودی کنترل دسترسی
hamming weight	وزن همینگ
patch	وصله
status	وضعیت
aggressive mode	وضعیت تهاجمی
adaptability	وفق‌پذیری
adaptive	وفقی
interruption	وقفه
virus	ویروس
stealth virus	ویروس پنهان
spy virus	ویروس جاسوس
polymorphic virus	ویروس چندچهره
metamorphic virus	ویروس دگردیس
boot sector virus	ویروس قطاع راه انداز
macro virus	ویروس کلان
memory-resident virus	ویروس مقیم در حافظه
attribute	ویژگی
completeness property	ویژگی تمامیت
complementation property	ویژگی مکملیت
homomorphism property	ویژگی هم‌ریختی
isomorphic	ویژگی یک‌ریختی

	property
ه	
هرزنامه	spam
هرزنامه نگار	spammer
هستار	entity
هستان شناسی	ontology
هسته	kernel
هشدار	alert
هم تراز	alignment
همبستگی	correlation
همبستگی متقابل	cross correlation
همبستگی هشدارها	alert correlation
هم‌پوشانی	overlap
هم‌روند	concurrent
همزمان، همگام	synchronous
همسازی، همخوانی	consistency
همگن	homogeneous
همه جا حاضر	omnipresent
همیشه مُعتَمَد	always trusted
ی	
یای انحصاری	exclusive OR (XOR)
یکپارچگی پیام	message integrity
یکپارچگی داده پیام	data message integrity
یکپارچگی، تمامیت	integrity
یکپارچه سازی	integration
یک‌نوا	monotone
یکه، واحد	unit
DES سه‌گانه	triple DES
m- رجعت‌پذیر	m-resilient
MIPS-سال	MIPS-year
NP- تمام	NP-complete
NP-سخت	NP-hard
r-برخورد	r-collision

منابع:

۱- اصول امنیت شبکه‌های کامپیوتری، کاربردها و استانداردها، ویلیام استالینگ، ترجمه مسعود موحد، نشر پیام رسان، زمستان ۱۳۸۵.

۲- مبانی امنیت فضای رایانه‌ای، محمد جعفری، نشر علوم پایه، تابستان ۸۵.

۳- مقدمه‌ای به امنیت شبکه داخلی، شهریار بیژنی و حسین کرامتی، پژوهشکده پردازش علائم هوشمند، ۱۳۸۳.

۴- جنگ اطلاعات و امنیت، ترجمه شیخ زادگان، حسین نژاد، روحانی، پژوهشکده پردازش علائم هوشمند، ۱۳۸۳

۵- نقش توابع درهم‌ساز در رمزنگاری و امنیت، مجید نادری و معصومه صفخانی، دانشگاه علم وصنعت ایران، ۱۳۸۷.

۶- نظریه‌های امنیت، علی عبدالله خانی، تهران، فروردین ۸۳

۷- مبانی امنیت شبکه، شرکت ایز ایران و جهاد دانشگاه صنعتی شزیف، اریک مایوالد، پاییز ۱۳۸۵.

۸- نفوذگری در شبکه و روش‌های مقابله، پدیدآورنده: احسان ملکیان، ویراسته : شکیبا ضیایی و هادی پیشرفت ، ناشر: نص، تابستان ۱۳۸۵.

۹- فنآوری اطلاعات- واژه‌ها و اصطلاحات- قسمت هشتم: امنیت، سعید حسینی خیاط وهمکاران، موسسه استاندارد و تحقیقات صنعتی ایران، بهمن ۱۳۸۶.

۱۰- فرهنگ تشریحی واژگان امنیت فناوری اطلاعات، گردآوری وترجمه موسسه روشنگران اندیشه، نشر موسسه آموزشی و تحقیقاتی صنایع دفاعی- طرح فراسازمانی فاوا، تابستان ۱۳۸۶.

۱۱- اصول امنیت سیستم‌ها و شبکه‌های رایانه‌ای، شهرام بختیاری و سعید قاضی مغربی انتشارات دانشگاه صنعتی شریف، ۱۳۸۵.

۱۲- فرهنگ تشریحی واژه‌ها و اصطلاحات کامپیوتری مایکرو سافت، مترجم سعید ظریفی مؤسسه فرهنگی هنری دیباگران تهران .

۱۳-راهنمای امنیت فناوری اطلاعات، جورج سادوکای و همکاران، ترجمه مهدی میردامادی، زهرا شجاعی، محمد جواد صمدی، شورای عالی اطلاع رسانی، ۱۳۸۴.

۱۴-شبکه های کامپیوتری، اندروس اس.تنن‌بام، ترجمه حسین پدرام، احسان ملکیان، علی رضا زارع پور، انتشارات نص، چاپ ششم، ۱۳۸۵.

۱۵- مقدمه‌ای بر رمزنگاری، ج.ا باخمن، ترجمه مرتضی اسماعیلی، انتشارات دانشگاه صنعتی اصفهان، ۱۳۸۳.

۱۶-واژه‌های رایانه و فناوری اطلاعات، مصوب فرهنگستان ادب و زبان فارسی، خرداد ۱۳۸۶.

۱۷- واژه‌نامه مخابرات، ویرایش سوم، گروه واژگان طرح استانداردهای ملی مخابرات، مرکز تحقیقات مخابرات.

۱۸- واژه‌های مخابرات، مصوب فرهنگستان زبان وادب فارسی، بهمن ۱۳۸۷.

۱۹- مجموعه مقالات کنفرانس‌های رمز، دوره اول تا دور ششم.

۲۰- ده‌ها پایان‌نامه کارشناسی ارشد و دکترا در زمینه رمز و امنیت اطلاعات.

21. Handbook of Applied Cryptography, Menezes, A.J., P.C. van Oorschot, and S.A. Vanstone, CRC Press, Boca Raton, FL, 1997.
22. Encyclopedia of Cryptography and Security, Edited by Henk C. A. van Tilborg, Springer Science, 2005.
23. Handbook of Database security Applications and Trends edited by MichaelGertz, SushilJajodia, SpringerScience,2008.
24. Encyclopedia of cryptology, David E. Newton, ABC-CLIO, California 1997.
25. Microsoft Encyclopedia of Security, Mitch Tulloch. , Microsoft Press, 2003.
26. Dictionary of Information Security, Robert Slade, Syngress, 2006.
27. ISO/IEC 2382-8:1998, 2th Ed: information technology – Vocabulary – Part 8: Security.
28. National information systems security (INFOSEC) GLOSSARY.
29. Glossary of Key Information Security Terms, NIST IR 7298, Richard Kissel, April 2006.
30. Applied Cryptography, Bruce Schneier, second edition, John Wiley, 1996.
31. Modern Cryptography: theory and practice, Webno Mao, Prentice Hall, 2004.
32. Network Security Essentials: Application and Standards, William Stallings,Prentice Hall,1999.
33. Information Security Glossary, Primode, March 2003.
34. National Information Assurance (IA) Glossary, Keith B. Alexander, Revised June 2006.
35. http://www.wikipedia.org.
36. http://www.yourwindow.to/information-security/index.htm.
37. http://www.ciphersbyritter.com/GLOSSARY.HTM.
38. http://www.businesslink.gov.uk.
39. http://www.itsecurity.com/security.htm?s=93.
40. http://www.pki.vt.edu/help/glossary.html.
41. http://www.rsa.com/rsalabs/node.asp?id=2373.
42. http://tldp.org/HOWTO/Apache-WebDAV-LDAP-HOWTO/glossary.html.
43. http://download.oracle.com/docs/cd/A58617_01/network.804/a54088/gls.htm#423707.