English	Español
abuse	abuso
access control	control de acceso
acquirer	adquirente
adaptive attack	ataque adaptante
adversary	adversario
affine function	la función afine
API (Application Programming Interface)	Interfaz De Programación De Uso
asymmetric cryptography, public key cryptography	criptografía asimétrica, criptografía dominante pública
attack	ataque
audit	intervención
authentication	autentificación
authorization	autorización
availability	disponibilidad
avalanche criterion	criterio de la avalancha
balanced Boolean function, binary balanced function	función boleana equilibrada, función equilibrada binaria
balancedness	
BAN (Burroughs, Abadi, Needham) logic	lógica BAN
bent function	función doblada
binding	el atar (tying)
biometric device	dispositivo biométrico
biometric	biométrico
birthday attack	ataque del cumpleaños
birthday paradox	paradoja del cumpleaños

bit commitment	comisión del bitio
blind signature	firma oculta
blinding	el cegar
block cipher	cifra del bloque
brute-force attack, exhaustive attack	ataque de la bruto-fuerza, búsqueda exhaustiva
bug	bug, bicho, gazapo, error lógico, fallo lógico

CBC (cipher block chaining)	modo CBC, encadenamiento del bloque de la cifra
card issuer	emisor de la tarjeta
certificate	Certificado
certificate of primality	certificado del primality
certification authority	autoridad de la certificación (AC)
certificate repository	depósito del certificado
CRL (certificate revocation list)	lista de la revocación del certificado
CFB (cipher feedback)	realimentación de la cifra
challenge	Desafío
challenge-response protocol	protocolo de la desafiar-respuesta
checksum	suma de comprobación
Chinese Remainder Theorem (CRT)	Teorema Chino Del Resto
chosen plaintext attack	ataque elegido del plaintext
ciphering	el cifrar
cipher strength	fuerza de la cifra
ciphertext	texto cifrado
ciphertext only attack	ataque del texto cifrado

	solamente
classified	Clasificado
collision resistance	resistencia de la collision
commercial security	eguridad comercial
completeness	lo completo
compromise	compromiso
computational security	seguridad de cómputo
computationally infeasible, intractable	de cómputo infeasible, insuperable
computer network security	seguridad de la red de ordenadores
confidentiality	secreto
confusion	confusión
correlation immunity	inmunidad de la correlación
covert channel	canal secreto
cracker	descifrador
cross-certification	Cruz-certificación
cryptanalysis	Criptoanálisis
cryptoalgorithm	Algoritmo criptográfico
cryptographic area	Area criptográfica
cryptographic check value	valor del cheque criptográfico
cryptographic device	dispositivo criptográfico
cryptographic equipment	equipo criptográfico
cryptographic module	módulo criptográfico
cryptography	criptografía
cryptology	criptología
cryptosystem	Sistema criptografía
cut and choose (protocol)	corte y elija (protocolo)

DEK (Data Encryption Key)	Clave codifique de datos
data integrity	integridad de datos
data origin authentication	autentificación del origen de datos
data protection	protección de los datos
decipherment, decryption	Desciframiento
dedicated hash function	función dedicada del hash
dictionary attack	ataque del diccionario
discrete logarithm	logaritmo discreto
differential cryptanalysis	criptoanálisis diferenciado
diffusion	difusión
digital notary	notario digital
digital signature	firma digital
digital signature law	Ley de firma digital
distinguishing identifier	identificador que distingue
distinguished name	nombre distinguido
domain	dominio
DRC (Data Recovery Center)	Centro De Recuperación De los Datos
dual signature	Firma dual

eavesdropping	el escuchar detras de las puertas, espionaje
ECB (electronic code	libro electrónico del

book)	código
EDI (electronic data interchange)	intercambio de los datos electrónicos, intercambio de datos informatizados, intercambio electrónico de datos
electronic cash	Dinero electrónico, digital, virtual
electronic commerce	comercio electrónico, comercio en línea, comercio virtual, comercio por Internet
electronic payments	pago electrónico
elliptic curve	curva elíptica
elliptic curve cryptosystem (ECC)	Sistema criptografía de la curva elíptica
elliptic curve discrete logarithm	logaritmo discreto de la curva elíptica
encipherment, encryption	Cifrado
entity authentication	autentificación de la entidad
exhaustive (key space) attack	ataque exhaustivo (del espacio dominante)
exponent	exponente

factorization / factoring	Facturización / el descomponer en factores
fault injection	inyección del defecto
feedback shift register	Registro de cambio realimentación
fingerprint	huella digital
firewall	cortafuego

frequency analysis	análisis de frecuencia

hacker	Pirata(o) informática(o), hacker
hardware	Hardware, soporte
hash function	función del hash
hash value, hash code	Valor hash, código hash
HEART (Hybrid Encryption, Authentication and non-Repudiation Transcoder)	Cifrado, autentificación y no-Renegación híbridos Transcoder
home banking	actividades bancarias caseras

identification	identificación
impersonation, masquerade	personificación, masquerade
initial value	valor inicial
initialisation vector (IV)	vector de la inicialización
instance hiding computation, blind computation	cómputo que oculta del caso, cómputo oculto
integrity	integridad
interception	interceptación
interleaving attack	Ataque de interpolación
iterated block cipher	Cifra bloque iterada
ITSEC (Information Technology Security Evaluation Criteria)	Criterios De la Evaluación De Seguridad De la Tecnología De Información

KEK (Key Encryption	Llave Cifrado de la

Key)	Llave
key	Llave, clave
key agreement	Acuerdo de la llave
key archival	Archival de la llave
key backup	Copia de seguridad de la llave
key distribution	Distribución de las llaves
Key Distribution Center (KDC)	Centro de distribución de las llaves
key escrow	Fideicomiso de las llaves
key escrow cryptography	Criptografía del fideicomiso de las llaves
key establishment	Llave establecido
key exchange	Cambio de las llaves
key generation	Generación de las llaves
key management	Gerencia de llaves
key recovery	Recuperación de la llave
key scheduling	el programar de llaves
key stream	Torrente de llaves
key transport	Transporte de llaves
key validation	Validación de la llave
knapsack problem	problema de la mochila
known plaintext attack	Ataque de plaintext sabido

law enforcement	aplicación de ley, policía
LEAF (law enforcement access field)	campo del acceso de la aplicación de ley

linear complexity, linear span	complejidad linear, palmo linear
linear cryptanalysis	criptoanálisis linear
linear function	función linear
MAC (message authentication code)	código de la autentificación del mensaje
man-in-the-middle attack	ataque hombre en el medio
masquerade, impersonation	masquerade, personificación
MDC (Modification Detection Code)	Código De la Detección De la Modificación
meet in the middle attack	Ataque reunión en el medio
merchant	comerciante
message	mensaje
message authentication	autentificación del mensaje
message digest	resumen del mensaje
mode of operation	modo de operación
modular arithmetic	aritmética modular
modulus	módulo
monoalphabetic cipher	Cifra alfabética solo
multiparty computation	
multiple encipherment	Cifrado múltiple
mutual authentication	autentificación mutua

nonce	
nonlinearity	deslinearidades
non-repudiation	No renegación

notary	notario
NSA (National Security Agency)	Agencia De la Seguridad Nacional, ASN (Always Say Nothing)
Number Field Sieve	Tamiz Del Campo Del Número
number theory	teoría del número

oblivious transfer	transferencia olvidadiza
OFB (output feedback)	Realimentación de la salida
one-time pad	cojín de una sola vez
one-way function	función unidireccional
on-line password guessing attack	Ataque del conjeturar de la contraseña en línea

pad	cojín
padding	acolchado
password	contraseña
PCMCIA card, PC card	
PEM (Privacy Enhanced Mail)	
perfect nonlinear function	función no lineal perfecta
perfect secrecy	secreto perfecto
permutation	permutación
PGP (Pretty Good Privacy)	software de encriptación PGP, soporte lógico de encriptación PGP
PIN (Personal Identification Number)	número de identificación personal

PKI (Public Key Infrastructure)	ICP (infraestructura de claves públicas)
plaintext	
policy	política
polyalphabetic cipher	cifra alfabética múltiple
preimage resistance	
2nd preimage resistance	
primality test	prueba del primality
prime (number)	Primo, el número primo
privacy	intimidad
private key	llave privada
proactive cryptography	
probabilistic encryption	cifrado probabilistic
product cipher	cifra del producto
propagation criterion	criterio de la propagación
proprietary cipher	cifra propietaria
provably secure	demostrable asegure
prover	demostrador
pseudoprime (number)	Pseudoprima, seudoprima
pseudorandom	pseudoaleatorio
public key	llave pública
public key cryptosystem	sistema criptografía dominante público

quadratic sieve	tamiz cuadrático
quantum computer	computadora del quántum

quantum cryptography	criptografía del quántum

random	al azar, aleatorio
randomizer	Seleccionador al azar
redundancy	redundancia
reflection attack	ataque de la reflexión
registration authority	autoridad del registro
related key attack	ataque llave relacionada
replay attack	Ataque de repitición
reverse engineering	ingeniería reversa
revocation	revocación
risk analysis	análisis del riesgo
root certification authority	autoridad certificación de la raíz
round function	función redonda

salt	Sal
SAM (Secure Application Module)	Asegure El Módulo De Uso
S-box	
secrecy	secreto
secret key	llave secreta
secret sharing	el compartir secreto
secure envelope	asegure el sobre
secure messaging	asegure la mensajería
security	seguridad
security layer	capa de la seguridad
security mechanism	mecanismo de la seguridad

security module (SM)	módulo de la seguridad
security policy	política de la seguridad
security service	servicio de seguridad
seed	semilla
semantic security	seguridad semántica
semi-bent function	semi-doblo' la función
sender	envíedor
session key	llave de la sesión
shortcut attack	ataque del atajo
signature	La firma
signature scheme	esquema de la firma
signature verification	verificación de la firma
signing	firma
smart card	tarjeta electrónica
software	software
S-P Network	red de la substitución-permutación
spoof	broma
spread spectrum	separe el espectro
standard	El criterio
stand-alone	independiente
steganography, disappearing cryptography, information hiding, obfuscation techniques	Steganografía, criptografía que desaparece, el ocultar de la información, técnicas de la ofuscación
stream cipher	cifra de la corriente
strict avalanche criterion (SAC)	criterio terminante de la avalancha
strong authentication	autentificación fuerte

strong primes	Primos fuertes
subliminal channel	canal subconsciente
substitution	substitución
symmetric cryptography, classical cryptography	criptografía simétrica, criptografía clásica
system security officer	oficial de seguridad del sistema

tamper evident	pisón evidente
tamper proof	Ser resistente al pisón
tamper resistant	Ser resistente al pisón
TEMPEST	TEMPESTAD
threshold scheme	esquema del umbral
ticket	boleto
ticket-granting ticket (TGT)	boleto-conceder el boleto
timestamp	
timestamping (digital)	
timing attack	ataque que mide el tiempo
token	símbolo
traffic analysis	análisis de tráfico
trapdoor function	función del trapdoor
trapdoor one-way function	función de una forma del trapdoor
trusted third party (TTP)	tercero de confianza, tercera parte de confianza
Trojan horse	Trojan Horse, Caballo Trojan

undeniable signature	firma innegable
unpredictable	imprevisible
unconditional security	seguridad incondicional

verifier	verificador
virus	virus
visual cryptography	criptografía visual
VPN (Virtual Private Network)	Red Privada Virtual

weak key	llave débil
white noise	ruido blanco
wired logic card	tarjeta atada con alambre de la lógica
wiretap	wiretap
wiretapping	
web browser	Navegador de la web
work factor	factor del trabajo
workstation	Orenador personal
worm	gusano
WWW (World Wide Web)	La Web (WWW)

zero-knowledge proof/protocol	Prueba/protocolo del cero-conocimiento