Deutsch	english (USA)
(un)autorisiert	(un)authorized
(un)endlich	(in)finite
(un)erreichbar	(un)achievable
(un)erwünscht	(un)intended
(un)nötig	(un)necessary
(un)sicher	(in)secure
(un)vorhersagbar	(un)predictable
Abbildung	mapping
Abfragen	queries
Abhörer	interceptor
Abwehr	defense
Adaptivität	adaptivity
Adressierung	addressing
ahnden	punish
ähnlich	similar
allgemein	in general
allmächtig	omnipotent
also	therefore
Angestellter	employee
Angreifermodell	attacker model
Angreifersicht	view of attacker
angrenzend	neighboring
Angriffsbereich	area of attack
Angriffserfolg	succes of attack
Angriffstyp	type of attack
Angriffsziel	goal of attack
Anmerkung	note
Annahme	assumption
Anonymität	anonymity
Anordnung	arrangement
anrichten	inflict
Anschlussleitung	subscriber line
Anweisung	command
Anwendung	application
äquivalent	equivalent
aufdecken	reveal
Aufenthaltsinformation	roaming information
Aufruf	call
Aufwand	expense
Ausblick	outlook
Ausbreitung	propagation
auslassen	skip
Außenstehender	outsider
Ausweis	ID-card
Authentikationssystem	authentication system
bedeutungslos	dummy
bedeutungsvoll	meaningful
Bedingung	constraint
Bedrohung	threat
beglaubigen	certify
Behauptung	claim
Beispiel	example
beliebig	arbitrarily
Benutzer	user
beobachtend	observing

berücksichtigen	consider
beschränken	restrict
besorgen	get
bestehen	pass
bestimmen	determine
Betreiber	operator
Beweis	proof
beweisen	prove
Bildtelefon	videophone
Bitfolge	bit stream
Bitkette	bit string
Block	block
Breitband	broadband
bzgl.	concerning
bzw.	respectively
Chiffre	cipher
Chiffrierschlüssel	encryption key
Chinesischer Restsatz	Chinese Remainder Theorem
Chipkarte	smart card
Datenschutz	data protection
datenschutzfreundlich	privacy enhancing
dazulegen	append
Dechiffrierschlüssel	decryption key
Definitionsbereich	domain
Dienst	service
Diensterbringung	service delivery
disjunkt	disjoint
drahtlos	wireless
Durchschnitt	average
Effizienz	efficiency
Eigenschaft	property
eindeutig	unique
Eingriff	interference
einordnen	arrange
Einweg	one-way
einzeln	separate
Empfang	receiving
Empfänger	recipient
Ende-zu-Ende	end-to-end
Endgerät	terminal
Engpass	bottleneck
Entscheidung	decision
Entschlüsselung	decryption
entsprechend	appropriately
Entwerfer	designer
Entwicklung	development
erfordern	demand
ergeben	yield
Erinnerung	reminder
erkennbar	recognizable
Erlaubnis	permission
erreichbar	feasible
Erreichbarkeit	reachability
erwarten	await
es gilt	it holds
Etappe	stages

exponentiell	exponential
fähig	capable
faktorisieren	factor
Faktorisierung	factorization
Falle	trap
Fälschung	forgery
fehlend	missing
Fehlererkennung	fault detection
Fehlertolerance	fault tolerance
Fehlerwahrscheinlichkeit	error probability
Fernmeldesatellit	communications satellite
Fernsprechortsnetz	regional switched phone network
Fernvermittlungstelle	long-distance exchange
festlegen	commit
Fingerabdruck	finger print
folgen	follow
Folgerung	conclusion
Forderung	requirement
Freizeichen	dial tone
Funknetz	radio network
ganz rechts	rightmost
gdw.	iff
geeignet	adequate
geeignet	suitable
geflochten	braided
Gegenmaßnahme	countermeasure
geheim	secret
geheim halten	keep secret
gemäß	according to
genauer	more precise
genügend	sufficient
Gerät	device
gestört	corrupted
gewartet	maintained
gewünscht	desired
ggT	gcd
Glasvitrine	show-case
Glaubwürdigkeit	credibility
gleich	equal
Gleichverteilung	even distribution
Grenze	limit
größter gemeinsamer Teiler	greatest common divisor
Grundlagen	basic facts
Haftung	liability
Hersteller	manufacturer
höchstens	at most
Hörfunk	radio broadcast
Identifikation	identification
indeterministisch	probabilistic
Informationsgewinn	disclosure of information
informationstheoretisch	information theoretic
Inhalt	content
Instanz	entity
Interessendaten	data on interests
Integrität	integrity
Invertierung	inverting

juristische Regelung	legal provisions
Kabelverbindung	cabel link
Kanalkodierung	channel coding
Klartext	plaintext
Klartextmenge	set of plaintext
kollisionsresistent	collision-resistant
Komplexitätstheorie	complexity theory
Konzelation	concealment
Konzelationssystem	encryption system
Körper (math.)	field
Kryptographie	cryptography
längentreu	maintaining message length
Laufzeit	running time
leisten	provide
Leitungsnetz	wire network
liefern	provide
Lösung	solution
Maßnahme	measure
mehrseitig	multilateral
Menschen	human beings
Mittelwertbildung	mean calculation
Nachricht	message
Netzabschluss	network termination
nicht herumzeigbar	undeniable
Nutzdaten	message contents
offen	open
öffentlich	public
öffentlich bekannt	publicly known
Optimierung	improvement
Ortsvermittlungstelle	local exchange
OVSt	local exchange
Paarbeziehung	pair relation
Peilung	bearing
Periodenlänge	length of period
Polynom	polynomial
Prädiktor	predictor
präfix	prefix
Primzahl	prime number
probabilistisch	probabilistic
Produzent	producer
protokolltreu	truthful to protocol
puffern	batch
quadratischer Rest	quadratic residue
Quittung	receipt
raten	guess
Rechnernetze	computer networks
Rechtssicherheit	legal certainty
Restklassenring	ring of residue classes
Reziprozitätsgesetz	quadratic law of reciprocity
Rückkopplung	feedback
Rücksicht	consideration
Satz (math.)	theorem
schalenförmig	shell-shaped
schätzen	estimate
scheinbar	seemingly
Schicht	layer

Schieberegister	shift register
Schirmung	shielding
Schlüsselaustausch	key exchange
Schlüsselgenerierung	key generation
Schlüsselmenge	set of keys
Schlüsseltext	ciphertext
Schlüsselverteilung	key exchange
Schlüsselwert	key value
Schnappschloss	spring lock
Schreibzugriff	write access
schubweise	batch-wise
Schutzmechanismen	protection measures
Schutzziel	protection goal
schwächen	weaken
Schwellwert	threshold
Selbstwählferndienst	subscriber trunk dialing
Sicherheit	security
Sicherheitsklassen	security classes
Siegel	seal
sinken	decrease
sinnvoll	useful
Skizze (i.S.v. Entwurf)	sketch
Speicher	memory
Startwert	initial value
Suchprinzip	principle of search
Teil	part
teilerfremd	coprime
Teilnehmer	participant
Teinehmerendgerät	terminal equipment
Testergebnis	test result
Treuhänder	trustee
trickreich	skillfull
Trojanisches Pferd	trojan horse
Trugschluss	fallacy
Übereinstimmung	correspondence
überlagern	superpose
Überlagerung	superposition
Übertragungssystem	transmission system
Umbenennung	renaming
umcodieren	re-encrypt
Umfeld	circumstance
umgekehrt	converse
umkehrbar	reversible (Vorgang), invertible (Funktion, Permutation)
Umlauf	circulation
umsortieren	change order
umständlich	cumbersome
unabhängig	independently
unbedingt	unconditional
Unbeobachtbarkeit	unobservability
undurchsichtig	opaque
unentscheidbar	undecidable
unerfüllbar	cannot hold
unerheblich	irrelevant
ungerade	odd
unterscheiden	distinguish
Unverkettbarkeit	unlinkability

Ur-	initial
Verallgemeinerung	generalization
verändernd	modifying
Verankerung	anchoring
Verbesserung	improvement
Verbindlichkeit	legal enforceability
Verbindungsverschlüssung	link encryption
verdeckt	hidden / covert
verdeckt	invisible
Verdecktheit	hiding
Verfügbarkeit	availability
vergleiche, vgl.	compare
Verhalten	behavior
Verkehrsdaten	traffic data
verkürzt	truncated
Vermittlungsnetz	switched network
Vermittlungsstelle	telephone exchange
veröffentlichen	publish
verschieden	different
verschwindender Bruchteil	infinitesimal fraction
Verschlüsselung	encryption
Verschmutzung	pollution
verstärken	strengthen
verteilte Systeme	distributed systems
Verteilung	broadcast
Vertrauensbereich	domain of trust
vertrauenswürdig	thrustworthy
vertraulich	confidential
Vertraulichkeit	confidentiality
verwendbar	useable
verzögern	delay
Verzögerung	delay
von-Neumann-Rechner	von-Neumann-computer
Vorteil	advantage
wählen	choose
Wahrscheinlichkeit	probability
Wartungsdienst	service and maintenance
Wechselwirkung	correlation
wenig untersucht	somewhat analyzed
Wert	value
Wertebereich	co-domain
Widerspruch	contradiction
wie oben	as mentioned above
wohluntersucht	well analyzed
Wurzel	root
wurzelziehen	extracting roots
Zahlentheorie	number theory
Zahlungssystem	payment system
Zeichen	character
Zeichenkette	character string
Zeitabstand	interval
Zeitscheibenkanal	time-slice channel
Zerlegung	decomposition
Zeuge	witness
Ziel	aim

Zufallszahl	random number
Zugangskontrolle	admission control
Zugriff	access
Zugriffskontrolle	access control
zuordnen	assign
zur Zeit	at present
Zurechenbarkeit	accountability
zusammen passen	fit
Zusammenfassung	summary
Zusammenhang	connectedness
Zwischen-	intermediate

english (USA)	Deutsch
(in)finite	(un)endlich
(in)secure	(un)sicher
(un)achievable	(un)erreichbar
(un)authorized	(un)autorisiert
(un)intended	(un)erwünscht
(un)necessary	(un)nötig
(un)predictable	(un)vorhersagbar
access	Zugriff
access control	Zugriffskontrolle
according to	gemäß
accountability	Zurechenbarkeit
adaptivity	Adaptivität
addressing	Adressierung
adequate	geeignet
admission control	Zugangskontrolle
advantage	Vorteil
aim	Ziel
anchoring	Verankerung
anonymity	Anonymität
append	dazulegen
application	Anwendung
appropriately	entsprechend
arbitrarily	beliebig
area of attack	Angriffsbereich
arrange	einordnen
arrangement	Anordnung
as mentioned above	wie oben
assign	zuordnen
assumption	Annahme
at most	höchstens
at present	zur Zeit
attacker model	Angreifermodell
authentication system	Authentikationssystem
availability	Verfügbarkeit
average	Durchschnitt
await	erwarten
basic facts	Grundlagen
batch	puffern
batch-wise	schubweise
bearing	Peilung
behavior	Verhalten
bit stream	Bitfolge
bit string	Bitkette
block	Block
bottleneck	Engpass
braided	geflochten
broadband	Breitband
broadcast	Verteilung
cabel link	Kabelverbindung
call	Aufruf
cannot hold	unerfüllbar
capable	fähig
certify	beglaubigen
change order	umsortieren
channel coding	Kanalkodierung

character	Zeichen
character string	Zeichenkette
Chinese Remainder Theorem	Chinesischer Restsatz
choose	wählen
cipher	Chiffre
ciphertext	Schlüsseltext
circulation	Umlauf
circumstance	Umfeld
claim	Behauptung
co-domain	Wertebereich
collision-resistant	kollisionsresistent
command	Anweisung
commit	festlegen
communications satellite	Fernmeldesatellit
compare	vergleiche, vgl.
complexity theory	Komplexitätstheorie
computer networks	Rechnernetze
concealment	Konzelation
concerning	bzgl.
conclusion	Folgerung
confidential	vertraulich
confidentiality	Vertraulichkeit
connectedness	Zusammenhang
consider	berücksichtigen
consideration	Rücksicht
constraint	Bedingung
content	Inhalt
contradiction	Widerspruch
converse	umgekehrt
coprime	teilerfremd
correlation	Wechselwirkung
correspondence	Übereinstimmung
corrupted	gestört
countermeasure	Gegenmaßnahme
credibility	Glaubwürdigkeit
cryptography	Kryptographie
cumbersome	umständlich
data on interests	Interessendaten
data protection	Datenschutz
decision	Entscheidung
decomposition	Zerlegung
decrease	sinken
decryption	Entschlüsselung
decryption key	Dechiffrierschlüssel
defense	Abwehr
delay	verzögern
delay	Verzögerung
demand	erfordern
designer	Entwerfer
desired	gewünscht
determine	bestimmen
development	Entwicklung
device	Gerät
dial tone	Freizeichen
different	verschieden
disclosure of information	Informationsgewinn

disjoint	disjunkt
distinguish	unterscheiden
distributed systems	verteilte Systeme
domain	Definitionsbereich
domain of trust	Vertrauensbereich
dummy	bedeutungslos
efficiency	Effizienz
employee	Angestellter
encryption	Verschlüsselung
encryption key	Chiffrierschlüssel
encryption system	Konzelationssystem
end-to-end	Ende-zu-Ende
entity	Instanz
equal	gleich
equivalent	äquivalent
error probability	Fehlerwahrscheinlichkeit
estimate	schätzen
even distribution	Gleichverteilung
example	Beispiel
expense	Aufwand
exponential	exponentiell
extracting roots	wurzelziehen
factor	faktorisieren
factorization	Faktorisierung
fallacy	Trugschluss
fault detection	Fehlererkennung
fault tolerance	Fehlertolerance
feasible	erreichbar
feedback	Rückkopplung
field	Körper (math.)
finger print	Fingerabdruck
fit	zusammen passen
follow	folgen
forgery	Fälschung
gcd	ggT
generalization	Verallgemeinerung
get	besorgen
goal of attack	Angriffsziel
greatest common divisor	größter gemeinsamer Teiler
guess	raten
hidden / covert	verdeckt
hiding	Verdecktheit
human beings	Menschen
ID-card	Ausweis
identification	Identifikation
iff	gdw.
improvement	Optimierung
improvement	Verbesserung
in general	allgemein
independently	unabhängig
infinitesimal fraction	verschwindender Bruchteil
inflict	anrichten
information theoretic	informationstheoretisch
initial	Ur-
initial value	Startwert
integrity	Integrität

interceptor	Abhörer
interference	Eingriff
intermediate	Zwischen-
interval	Zeitabstand
inverting	Invertierung
invisible	verdeckt
irrelevant	unerheblich
it holds	es gilt
keep secret	geheim halten
key exchange	Schlüsselaustausch
key exchange	Schlüsselverteilung
key generation	Schlüsselgenerierung
key value	Schlüsselwert
layer	Schicht
legal certainty	Rechtssicherheit
legal enforceability	Verbindlichkeit
legal provisions	juristische Regelung
length of period	Periodenlänge
liability	Haftung
limit	Grenze
link encryption	Verbindungsverschlüssung
local exchange	Ortsvermittlungstelle
local exchange	OVSt
long-distance exchange	Fernvermittlungstelle
maintained	gewartet
maintaining message length	längentreu
manufacturer	Hersteller
mapping	Abbildung
mean calculation	Mittelwertbildung
meaningful	bedeutungsvoll
measure	Maßnahme
memory	Speicher
message	Nachricht
message contents	Nutzdaten
missing	fehlend
modifying	verändernd
more precise	genauer
multilateral	mehrseitig
neighboring	angrenzend
network termination	Netzabschluss
note	Anmerkung
number theory	Zahlentheorie
observing	beobachtend
odd	ungerade
omnipotent	allmächtig
one-way	Einweg
opaque	undurchsichtig
open	offen
operator	Betreiber
outlook	Ausblick
outsider	Außenstehender
pair relation	Paarbeziehung
part	Teil
participant	Teilnehmer
pass	bestehen
payment system	Zahlungssystem

permission	Erlaubnis
plaintext	Klartext
pollution	Verschmutzung
polynomial	Polynom
predictor	Prädiktor
prefix	präfix
prime number	Primzahl
principle of search	Suchprinzip
privacy enhancing	datenschutzfreundlich
probabilistic	indeterministisch
probabilistic	probabilistisch
probability	Wahrscheinlichkeit
producer	Produzent
proof	Beweis
propagation	Ausbreitung
property	Eigenschaft
protection goal	Schutzziel
protection measures	Schutzmechanismen
prove	beweisen
provide	leisten
provide	liefern
public	öffentlich
publicly known	öffentlich bekannt
publish	veröffentlichen
punish	ahnden
quadratic law of reciprocity	Reziprozitätsgesetz
quadratic residue	quadratischer Rest
queries	Abfragen
radio broadcast	Hörfunk
radio network	Funknetz
random number	Zufallszahl
reachability	Erreichbarkeit
receipt	Quittung
receiving	Empfang
recipient	Empfänger
recognizable	erkennbar
re-encrypt	umcodieren
regional switched phone network	Fernsprechortsnetz
reminder	Erinnerung
renaming	Umbenennung
requirement	Forderung
respectively	bzw.
restrict	beschränken
reveal	aufdecken
reversible (Vorgang), invertible (Funktion, Permutation)	umkehrbar
rightmost	ganz rechts
ring of residue classes	Restklassenring
roaming information	Aufenthaltsinformation
root	Wurzel
running time	Laufzeit
seal	Siegel
secret	geheim
security	Sicherheit
security classes	Sicherheitsklassen
seemingly	scheinbar
separate	einzeln

service	Dienst
service and maintenance	Wartungsdienst
service delivery	Diensterbringung
set of keys	Schlüsselmenge
set of plaintext	Klartextmenge
shell-shaped	schalenförmig
shielding	Schirmung
shift register	Schieberegister
show-case	Glasvitrine
similar	ähnlich
sketch	Skizze (i.S.v. Entwurf)
skillfull	trickreich
skip	auslassen
smart card	Chipkarte
solution	Lösung
somewhat analyzed	wenig untersucht
spring lock	Schnappschloss
stages	Etappe
strengthen	verstärken
subscriber line	Anschlussleitung
subscriber trunk dialing	Selbstwählferndienst
succes of attack	Angriffserfolg
sufficient	genügend
suitable	geeignet
summary	Zusammenfassung
superpose	überlagern
superposition	Überlagerung
switched network	Vermittlungsnetz
telephone exchange	Vermittlungsstelle
terminal	Endgerät
terminal equipment	Teinehmerendgerät
test result	Testergebnis
theorem	Satz (math.)
therefore	also
threat	Bedrohung
threshold	Schwellwert
thrustworthy	vertrauenswürdig
time-slice channel	Zeitscheibenkanal
traffic data	Verkehrsdaten
transmission system	Übertragungssystem
trap	Falle
trojan horse	Trojanisches Pferd
truncated	verkürzt
trustee	Treuhänder
truthful to protocol	protokolltreu
type of attack	Angriffstyp
unconditional	unbedingt
undecidable	unentscheidbar
undeniable	nicht herumzeigbar
unique	eindeutig
unlinkability	Unverkettbarkeit
unobservability	Unbeobachtbarkeit
useable	verwendbar
useful	sinnvoll
user	Benutzer
value	Wert

videophone	Bildtelefon
view of attacker	Angreifersicht
von-Neumann-computer	von-Neumann-Rechner
weaken	schwächen
well analyzed	wohluntersucht
wire network	Leitungsnetz
wireless	drahtlos
witness	Zeuge
write access	Schreibzugriff
yield	ergeben