English to hindi dictionary:

English	Hindi
Abuse	burā bartāva
Access control	abhigama niyantraṇa
acquirer	adhigrāhaka
adaptive attack	
adversary	virōdhī,
affine function	
Application Programming Interface	anuprayōga prōgrāmana antarāphalaka
asymmetric cryptography, public key cryptography	Asanyamita gūṛhalēkhana
attack	dhāvā
audit	lēkhā parīkṣaṇa
authentic	satyāpana
authorization	prādhikaraṇa
availability	prāpyatā
Avalanche criterion	Avalanche(O) mānadaṇḍa

Balanced Boolean function	Santulita boolean(O) prakārya
balancedness	
BAN logic	BAN n'yāya śāstra
Bent function	
Binding	āvaśyaka
Biometric device	Biometric(O) yantra
birthday attack	Janmadina dhāvā
Birthday paradox	Janmadina asatyābhāsa
Bit commitment	ṭukaṛā(A) pratibad'dhatā
Blind signature	apratyakṣa hastākṣara
blinding	Andhakara(A)
Block cipher	guṭṭa (A)bīja lēkha
Brute-force attack,exhaustive attack	pūrṇa dhava
bug	
biometric	

CBC(cipher block chaining)	bīja lēkha ṭukaṛā śrṛṅkhalana(A)
card issuer	Patraka nikāsak(A)
certificate	pramāṇaka
certificate of primality	Maulikta ka pramanaka
Certification authority	pramāṇīkaraṇa adhikārī
Certificate repository	kōṣa ka pramanaka

CRL (certificate revocation list)	khaṇḍana sūcī ka pramanaka
CFB (cipher feedback)	bīja lēkha pratipuṣṭi(A)
challenge	āhvāna
challenge-response protocol	āhvāna Javābi ka ādarśa patra
checksum	jāñca yōga
Chinese Remainder Theorem (CRT)	Cīnī śēṣaphala pramēya
chosen plaintext attack	cunā hu'ā viśud'dha pāṭhya par dhava
ciphering	bīja lēkha likhna
Cipher strength	bīja lēkha ki śakti
ciphertext	bīja likhita pāṭha
Ciphertext only attack	bīja likhita pāṭha dhava(A)
classified	anuvarga
Collision resistance	muṭhabhēṛa pratirōdha
Commercial security	Vyāpārika surakṣitatā
completeness	sampūrṇatā
compromise	samajhautā
Computational security	abhikalanātmaka jaṭilatā ki surakṣitatā
computationally infeasible, intractable	Avaśya(A)
computer network security	Computer(R)
confidentiality	gōpanīyatā
confusion	sambhrama
correlation immunity	Sahasambandha svādhīnatā(A)
covert channel	āvṛta mārga
cracker	kampyūṭara mēṁ anādhikṛta pravēśa va chēṛakhānī karanē vālā (A)
cross-certification	Tiryaka pramāṇaka(A)
cryptanalysis	kūṭa-lēkhana viślēṣaṇa(A)
cryptoalgorithm	kūṭa-lēkhana ki kalanavidhi
cryptographic area	Pracchannālēkhī ka kṣētra
Cryptographic check value	
Cryptographic device	kūṭa-lēkhana ka yantra
Cryptographic equipment	kūṭa-lēkhana ka upakaraṇa
Cryptographic module	kūṭa-lēkhana ka ansh(A)
cryptography	kūṭa-lēkhana
cryptology	kūṭa-lēkhana ki vidhi
cryptosystem	kūṭa-lēkhana ki sāraṇī(A)
cut and choose (protocol)	

DEK (Data Encryption Key)	ādhāra-sāmagrī ko gupt bhasha mein likne ki kunji

data integrity	āṅkaṛā śucitā
data origin authentication	ādhāra-sāmagrī ka aarambhikita ka pramanakata
data protection	āṅkaṛā rakṣaṇa
decipherment, decryption	vikōḍana
dedicated hash function	samarpita drutānvēṣaṇa padavI(A)
dictionary attack	koSha dhava(A)
discrete logarithm	
differential cryptanalysis	
diffusion	phailAva
digital notary	aṅkīya ēkhāpatra pramāṇakārī
digital signature	aṅkīya hastākṣara
digital signature law	aṅkīya hastākṣara niyama
distinguishing identifier	Vikhyāta abhijñāpaka
distinguished name	Vikhyāta naam
domain	kShetra
DRC (Data Recovery Centre)	
dual signature	hastākṣara

eavesdropping	pracchanna śravaṇa
ECB (electronic code book)	
EDI (electronic data interchange)	
electronic cash	ilēkṭrŏnika(R) nakada
electronic commerce	ilēkṭrŏnika(R) vāṇijya
electronic payments	ilēkṭrŏnika(R) bhuktan
elliptic curve	vakra
elliptic curve cryptosystem (ECC	
elliptic curve discrete logarithm	
encipherment, encryption	
entity authentication	Sthiti pramāṇīkaraṇa
exhaustive (key space) attack	pūrṇa dhava(A)
exponent	Vyakhyātā

factorization / factoring	Anśa banana ki vidhi(R)
fault injection	
feedback shift register	
fingerprint	aṅgulī-cihna
firewall	Bachav hetu liye gaye nirnaye(R)
frequency analysis	āvṛti viślēṣaṇa

hacker	ghusapaiṭhiyā
hardware	. lōhē pītala ādi kī vastu'ēṁ(O)

hash function	Hash padavi
hash value, hash code	Hash mūlya
HEART (Hybrid Encryption, Authentication and non-Repudiation Transcoder)	
home banking	

identification	abhinirdhāraṇa
impersonation, masquerade	svāṅga
initial value	Prarambhik mula
initialisation vector (IV)	prārambhikīkaraṇa sadiśa
instance hiding computation, blind computation	apratyakṣa saṅgaṇanā
integrity	akhaṇḍitva
interception	aṭakāva
interleaving attack	antaḥpatraṇa dhava
iterated block cipher	bīja lēkha Dōharānā(R)
ITSEC (Information Technology Security Evaluation Criteria)	ITSEC(O)

KEK (Key Encryption Key)	
key	Kunji
key agreement	In context of key(kunji): sam’mati
key archival	purālēkha sañcikā
key backup	sahāyatā
key distribution	vitaraṇa
Key Distribution Center (KDC)	
key escrow	
key escrow cryptography	
key establishment	sthāpana,
key exchange	adalī badalī
key generation	utpatti
key management	prabandhana
key recovery	bahālī
key scheduling	sūcī mēṁ rakhanā
key stream	Dhāra(A)
key transport	Aava gaman
key validation	mān'yakaraṇa
knapsack problem	sipāhī kā jhōlā
known plaintext attack	Parichit viśud'dha pāṭhya par dhava(A)

law enforcement	niyama ka pravartana(A)
LEAF (law enforcement access field)	
linear complexity, linear span	jaṭilatā(R)
linear cryptanalysis	kūṭa-lēkhana ka viślēṣaṇa

linear function	Padavī(R)

MAC (message authentication code)	Sandesh ki pramāṇīkaraṇa sanhitā
man-in-the-middle attack	
MDC (Modification Detection Code)	Āśōdhana anusandhāna sanhita(R)
meet in the middle attack	
merchant	Vyapari
message	Sandesh
message authentication	Sandesh ka pramāṇīkaraṇa(A)
message digest	Sandesh saṅgraha
mode of operation	Vidhi
modular arithmetic	aṅkagaṇita(R)
modulus	
monoalphabetic cipher	Ek niyam se banaya gaya kuta lekh
multiparty computation	Parikalana(R)
multiple encipherment	
mutual authentication	paraspara kā pramāṇīkaraṇa

nonce	
nonlinearity	
non-repudiation	svIkAra karanA
notary	lekhApatra pramANakArI
NSA (National Security Agency)	
Number Field Sieve	
number theory	Anko ka sid'dhānta(A)

oblivious transfer	Bina jankari sthānāntara karanā(A)
OFB (output feedback)	punarnivēśa,
one-time pad	(O)
one-way function	(O)
on-line password guessing attack	(O)

Pad	mulāyama jīna(A)
Padding	jīna ityādi kī gaddī(A)
password	kūṭa śabda
PCMCIA card, PC card	PC patraka
PEM (Privacy Enhanced Mail)	(A)
perfect nonlinear function	
perfect secrecy	Purna guptatā
permutation	kramavaya,
PGP (Pretty Good Privacy)	(A)

PIN (Personal Identification Number)	
PKI (Public Key Infrastructure)	
plaintext	Visudhya padhya
policy	nīti
polyalphabetic cipher	
preimage resistance	(O)pratibandha
2nd preimage resistance	(O)
primality test	(O)
prime (number)	abhājya
privacy	gōpanīyatā
private key	Nijī kunji
proactive cryptography	(O) kuta lekhan
probabilistic encryption	sambhāvyatā
product cipher	(O)
propagation criterion	
proprietary cipher	svāmī sambandhī kuta lekhana(R)
provably secure	surakṣita(O)
prover	
pseudoprime (number)	chadma abhājya(R)
pseudorandom	chadma yādṛcchika
public key	Sārvajanika kunji
public key cryptosystem	

quadratic sieve	Dvighāta chalanī(O)
quantum computer	Pramātrā(O)
quantum cryptography	Pramātrā(O)

random	ākasmika
randomizer	
redundancy	nirārthakatā
reflection attack	Parāvartana dhava(R)
registration authority	ēkhārōpaṇa adhikārī
related key attack	Sambandhīt kunji dhava(O)
replay attack	(O)
reverse engineering	ulaṭa abhiyāntrikī
revocation	khaṇḍana
risk analysis	Khatarānak viślēṣaṇa
root certification authority	Mūla pramāṇīkaraṇa adhikari
round function	(O)

salt	Namak
SAM (Secure Application Module)	
S-box	S- sandūka

secrecy	guptatā
secret key	Gupt kunji
secret sharing	Gupt sahabhājana
secure envelope	Gupt liphāphā
secure messaging	surakṣita sandēśana
security	surakṣitatā
security layer	surakṣitatā ki parat
security mechanism	surakṣitatā ki yantrāvalī
security module (SM)	
security policy	surakṣitatā ki niti
security service	surakṣitatā ki sēvā
seed	bīja
semantic security	śabdārtha vijñāna surakṣitatā
semi-bent function	
sender	bhējanēvālā,
session key	Satra ki kunji
shortcut attack	
signature	hastākṣara
signature scheme	hastākṣara padvati
signature verification	hastākṣara sid'dhakaraṇa,
signing	
smart card	Smart patraka(O)
software	(O)
S-P Network	(O)
spoof	nirarthaka
spread spectrum	
standard	mānaka
stand-alone	Ātmanirbhara(A)
steganography, disappearing cryptography, information hiding, obfuscation techniques	Kuta lekhana ki kala
stream cipher	
strict avalanche criterion (SAC)	(O)
strong authentication	Purna pramāṇīkaraṇa(A)
strong primes	
subliminal channel	Aparyāpta praṇāla(A)
substitution	sthānāpanna karanā
symmetric cryptography, classical cryptography	(O)
system security officer	

tamper evident	n'yāya virud'dha(R)
tamper proof	kapaṭa prabandha se pare
tamper resistant	kapaṭa prabandha ka avarodhak
TEMPEST	Āndhī(A)
threshold scheme	Dēhalī padvati

ticket	(O)
ticket-granting ticket (TGT)	
timestamp	yantra
timestamping (digital)	
timing attack	
token	cihna
traffic analysis	Yātāyāta viślēṣaṇa
trapdoor function	(O)
trapdoor one-way function	(O)
trusted third party (TTP)	(O)
Trojan horse	Sahasi(O)

undeniable signature	akhaṇḍanīya hastākṣara
unpredictable	
unconditional security	Asambandha suraksha

verifier	pramāṇita karane wala
virus	chūta kē rōgōṁ kā viṣa(A)
visual cryptography	
VPN (Virtual Private Network)	(O)

weak key	Durbala kunji
white noise	
wired logic card	tāra yukta tarka śāstra patra(O)
wiretap	
wiretapping	
web browser	Jail vicaraka(O)
work factor	
workstation	
worm	kIDA, dhIre dhIre chhipakara kAma karanA
WWW (World Wide Web)	(O)

Zero knowledge proof/protocol	