

Contents

Articles

Electronic signature	1
Cryptography	9
Outline of cryptography	23
1dl	32
Anonymous veto network	33
Array controller based encryption	34
Authenticated encryption	36
Authorization certificate	37
Autokey cypher	39
Avalanche effect	42
Averaging argument	43
Backdoor (computing)	44
Bent function	47
Bigram	50
BLACKER	51
Blind credential	52
Blind signature	52
Blinding (cryptography)	55
Block design	56
Block size (cryptography)	59
Blom's scheme	60
BLS (cryptography)	62
Blum-Micali algorithm	63
Boneh/Franklin scheme	64
Boolean function	66
Brown fox code	67
Burrows–Abadi–Needham logic	68
Bus encryption	71
Byzantine fault tolerance	72
Cardan grille	74
Chaocipher	76
Cipher	77
Cipher runes	82
Ciphertext	84

ÚSTŘEDNÍ KNIHOVNA
právnícké fakulty MU
~~R-2069~~ / 151 580

PT-436

Ciphertext expansion	87
Ciphertext indistinguishability	87
Civision	90
Client-Side Encryption	90
Clipper chip	90
Cocks IBE scheme	92
Code (cryptography)	94
Code word	98
Codebook	99
Codress message	100
Collision resistance	100
Commitment scheme	101
Communications security	105
Comparison of cryptographic hash functions	108
Completeness (cryptography)	112
Compromise	112
Computer insecurity	113
Concrete security	119
Confusion and diffusion	120
Conjugate coding	121
Correlation attack	121
Correlation immunity	125
Cover (telecommunications)	126
Cover-coding	126
Critical Security Parameter	126
Crypto-politics	127
Cryptochannel	127
Cryptographic engineering	128
Cryptographic hash function	131
Cryptographic nonce	137
Cryptographic Service Provider	138
Cryptographic Test Correction	139
Portal:Cryptography	140
CrypTool	143
Cryptosystem	145
Cryptovirology	146
Decipherment	148
Deniable encryption	150

Designated verifier signature	153
Deterministic encryption	153
Digital credential	154
Digital signature	158
Digital signature forgery	165
Dining cryptographers problem	166
Diplomatic bag	168
Direct Anonymous Attestation	169
Discrete logarithm	171
EFF DES cracker	173
Elliptic curve cryptography	175
Encrypted function	181
Encryption	182
End-to-end encryption	183
Enigma machine	185
Entropic security	204
Ephemeral key	205
Factorization of polynomials over a finite field and irreducibility tests	205
Feedback with Carry Shift Registers	211
File camouflage	212
Floradora	213
Forking lemma	213
Forward anonymity	215
Friend-to-friend	215
Generic group model	219
Group key	220
Group signature	220
Group-based cryptography	222
HashClash	223
Homomorphic encryption	223
Horton Principle	226
Hybrid cryptosystem	227
Hyper-encryption	228
ID-based cryptography	229
ID-based encryption	230
Ideal lattice cryptography	234
Index of coincidence	241
Information leakage	246

Initialization vector	247
Kerckhoffs's Principle	249
Key (cryptography)	252
Key Ceremony	253
Key number method	255
Keyring (cryptography)	255
Kish cypher	255
Kiss (cryptanalysis)	258
Kleptography	258
Knapsack problem	259
KY-7	265
Lamport signature	265
Lattice-based cryptography	268
Lattice problem	271
Learning with errors	275
Link encryption	278
Malleability (cryptography)	278
Master/Session	279
MDS matrix	279
Mean Shortest Distance	280
Mental poker	283
Merkle signature scheme	287
Mimic function	289
Mix network	290
MMH-Badger MAC	290
Mulabhadra	297
Multicast encryption	298
Multiple encryption	300
Multivariate cryptography	301
Naor-Reingold Pseudorandom Function	303
NIPRNet	305
Normal basis	306
Nothing up my sleeve number	307
Off-line Root CA	308
One-time pad	309
One-way encryption	319
One-way function	320
Padding (cryptography)	323

Pairing	326
Passphrase	328
Password Authenticated Key Exchange by Juggling	331
Password psychology	333
Password strength	333
Password-based cryptography	343
Perfect forward secrecy	344
Permutation box	345
PGP word list	345
Pizzino	354
Plaintext	355
Polygraphic substitution	357
Privilege Management Infrastructure	358
Proof-of-work system	359
Protocol composition logic	362
Provable security	363
Proxy re-encryption	364
Pseudorandom ensemble	365
Public Key Name Service	366
Quantum Byzantine agreement	367
Quantum cryptography	371
Quantum key distribution	374
Rabin signature algorithm	384
Randomness	386
RED/BLACK concept	394
Ring signature	395
Russian copulation	396
S-box	396
S/MIME	398
Salt (cryptography)	400
Scrambler	402
Secure cryptoprocessor	405
Secure Hash Standard	407
Secure voice	407
Security association	409
Security engineering	410
Security parameter	413
Security through obscurity	414

Self-shrinking generator	418
Server gated cryptography	419
SFINKS	420
Signals intelligence	420
Signcryption	434
Sinople	436
SIPRNet	436
Snake oil (cryptography)	438
Software token	440
Spkac	441
Standard Model (cryptography)	442
Statistically close	443
Strong cryptography	443
Strong secrecy	445
Subliminal channels	446
Superincreasing sequence	448
Symmetric Boolean function	449
Symmetric key management	449
Tamper resistance	451
Terahash	454
Texas Instruments signing key controversy	455
Tokenization (data security)	456
Trace Zero Cryptography	457
Transient-key cryptography	460
Transmission security	462
Trapdoor function	463
Trusted Computing	464
Trusted third party	474
Two-way security	475
Undeniable signature	475
Unicity distance	476
Unknown key-share attack	478
Variably Modified Permutation Composition	478
Verifiable secret sharing	479
Visual cryptography	482
Vocoder	483
Voice inversion	494
WYSIWYS	495

X.1035	496
YAK (cryptography)	497
Yao's test	498

References

Article Sources and Contributors	499
Image Sources, Licenses and Contributors	510

Article Licenses

License	513
---------	-----