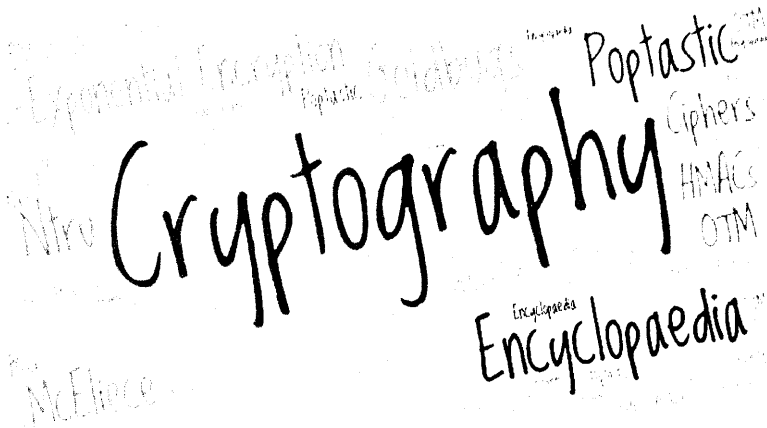

Linda A. Bertram
Gunther van Dooble
et al. *Editors*

Nomenclatura -

Encyclopedia of modern Cryptography and Internet Security:

From AutoCrypt and Exponential Encryption to Zero-Knowledge-Proof Keys



List of more than 330 Entries

Introduction

Linda A. Bertram and Gunther van Dooble:

Nomenclatura: What does a modern “Encyclopedia of Cryptography and Internet Security” offer for the education, discussion and sovereignty of learning professionals? - An interdisciplinary view on the Transformation of Cryptography: Fundamental concepts of Encryption, Milestones, Mega-Trends and sustainable Change in regard to Secret Communications and its Ideas, Key-Terms, Definitions and Good Practice.....17

Access Control	62	Authorization	79
AE - Adaptive Echo	62	AutoCrypt	80
AES - Advanced		Availability	80
Encryption Standard	63	Backdoor	81
AE-Token	66	Big Seven Study	
Algorithm	66	(2016)	84
Alice and Bob	68	Biometric Passport	85
Android	68	Birthday Problem	87
Anonymity	69	Blinding	88
Answer Method	70	Block Cipher	90
Asymmetric Calling	71	Bluetooth	92
Asymmetric		Botan	92
Encryption	71	Bouncy Castle	93
Attack	73	Broadcast (in	
Audit	74	Cryptography)	94
Authentication	77	Brute-force Attack	94

Bullrun (Decryption Program)	95	Cryptographic Discovery	117
Button	96	Cryptographic DNA	118
Buzz / e*IRC	96	Cryptographic Protocol	119
C/O - (Care-of)-Function	97	Cryptographic Routing	120
CBC - Cipher Block Chaining	97	Cryptographic Torrents	121
Caesar Cipher	98	Cryptography & Cryptology	122
Certificate Authority .	100	CryptoPad	123
Chaos Theory	101	Crypto-Parties	124
Cipher	102	CrypTool	125
Ciphertext	104	CSEK - Customer Supplied Encryption Keys	126
Ciphertext Stealing	105	Data Exposure	127
Clientside Encryption .	105	Data Obfuscation	127
C-Mail	106	Data Validation	128
Collision Attack	106	Database Encryption ..	128
Complexity	106	Decentralized Computing	130
Confidentiality	109	Delta Chat	130
Configuration	109	Democratization of Encryption	132
Congestion Control	109	Deniable Encryption ...	132
Continuous Improvement	109	DFA - Differential Fault Analysis	133
Corrective Action	111	DHT - Distributed Hash Table	134
Crawler	111		
Credential	111		
Cryptanalysis	112		
Crypto-Agility	114		
Cryptogram	114		
Cryptographic Calling	115		

Digest Access	
Authentication	134
Digital Signature	135
DNS - Domain Name	
System	137
Documented	
Information	138
Dooble Web Browser .	138
DTLS - Datagram	
Transport Layer	
Security	139
Eavesdropping	139
ECHELON	141
Echo (Protocol)	143
Echo Accounts	146
Echo Match	146
Echo-Grid	147
Echo-Network	148
Edgar Allan Poe	149
E-Government	150
ElGamal	152
Elliptic-Curve	
Cryptography	152
E-Mail Institution	154
Encapsulation	154
Encryption	155
Enigma Machine	155
Entropy	159
Ephemeral & Session	
Keys	159
EPKS - Echo Public Key	
Share Protocol.....	161
ETM - Encrypt-then-	
MAC.....	162
Exponential	
Encryption	164
Exponential Key	
Exchange	166
E2EE - End-to-End	
Encryption.....	167
Facial Recognition	
System	168
Fiasco Keys & Fiasco	
Forwarding	169
File-Encryptor	170
File-Sharing	170
Fingerprint	171
FinSpy	172
FireChat	173
Firewall	174
Flooding	175
Forward Secrecy	175
Forward-Secrecy-	
Calling	176
Freedom of Speech	176
Freenet	179
Full Echo	179
F2F - Friend-to-Friend	179
GCM - Galois/Counter	
Mode-Algorithm	180
Gemini	180

GnuPG - GNU Privacy	Information-
Guard 182	theoretic Security ... 199
Gnutella 182	Information Theory 199
Going the Extra Mile ... 182	Innovation 202
Goldbug (E-Mail	Instant Messaging 203
Password) 184	Institution 204
GoldBug (Software) 184	Integer Factorization .. 205
Goppa Code 185	Integrity 206
Graph-Theory 186	Internet 207
Group Chat 188	Internet Security 207
GUI - Graphical User	IPFS - Instant Perfect
Interface 189	Forward Secrecy..... 208
Half Echo 189	IRC – Internet Relay
Hash Function 190	Chat..... 209
HMAC - Keyed-Hash	Isomorphism 209
Message	Iterated Function 210
Authentication Code.. 191	Java 210
Homomorphic	Juggerknots /
Encryption 192	Juggerknot Keys 211
Homomorphic Secret	Juggernaut PAKE
Sharing 193	Protocol 212
HTTPS 193	KDF - Key Derivation
Human Rights 193	Function 214
Hybrid Encryption 196	Kerberos 215
Identification 197	Kerckhoffs' Principle .. 216
IMAP - Internet	Kernel 216
Message Access	Key 217
Protocol 197	Keyboard 218
Impersonator 197	Key Exchange /
Information Security .. 198	Establishment 218
	Key Size 223

Key Stretching	224	Monitoring	247
Keystroke Logging	226	Moore's Law	248
KeySync	227	Mosaic	248
Lattice-based		Multi-Encryption	249
Cryptography	227	Mutual	
Libcurl	229	Authentication	250
Libgcrypt	229	Neighbor	251
LibSpotOn	229	Netcat	251
Listener	230	Neuland	251
Login	230	NIST - National	
MAC - Message		Institute of Standards	
Authentication Code ..	230	and Technology	251
Magnet-URI	231	NOVA	252
Malleability	232	NTL - Number Theory	
Mass Surveillance	233	Library	252
Matrix	236	NTRU	252
Matryoshka Doll	237	Null Cipher	253
McEliece Algorithm ...	239	Number Theory	254
McNoodle Library	240	OFFSystem	255
Measurement	240	OMEMO	255
Media Bias	240	Open Source	256
MELODICA - Multi		OpenPGP - Open	
Encrypted Long		Pretty Good Privacy ...	256
Distance Calling	241	OpenSSH - Open	
Mesh Networking	242	Secure Shell	257
Meta-Data	244	OpenSSL - Open	
MITM – [Hu]Man-in-		Secure Sockets Layer ..	257
the-middle Attack	244	Opportunistic	
MITM - Meet-in-the-		Encryption	258
middle Attack	246	OTM - One-Time-	
Mix Network	247	Magnet	259

OTP - One-Time-Pad	259	Private Key	280
OTR - Off-the-Record	260	Private Servers	281
Ozone Address		Pseudorandom	
Postbox	260	Number Generator ..	281
Padding	261	Public Key Certificate ..	282
Pandamonium	262	Public Key	
Passphrase	263	Cryptography	283
Pass-through	263	PURE-FS - Pure	
Password	264	Forward Secrecy	284
Patch-Points	264	P2P - Peer-to-Peer	284
Pegasus Spyware	264	Qt	284
Pepper	265	Quantum Computing ..	285
Performance	266	Quantum	
PGP	266	Cryptography	285
Pigeonhole Principle ..	267	Quantum Information	
PKI - Public Key		Science	287
Infrastructure	268	Quantum Logic Gate ...	288
Plaintext	269	Rainbow Table	288
Plausible Deniability ..	270	Random	289
Point-to-Point	271	Random Number	
Policy	272	Generation	289
POP3 - Post Office		Raspberry Pi	292
Protocol	272	Remote Control	
POPTASTIC	273	Systems Spyware	292
PostgreSQL	274	REPLEO	293
Post-Quantum		Replay Attack	293
Cryptography	275	Requirement	294
PRISM (Surveillance		RetroShare	294
Program)	276	Review	295
Privacy	277	Rewind	295
Privacy Amplification ..	279	Rosetta-CryptoPad	295

ROT13	297	Smoke Crypto Chat	
Routing	298	App	316
RSA	299	SmokeStack	317
Salt, cryptographic	299	SMTPS - Simple Mail	
SCTP - Stream Control		Transfer Protocol	
Transmission		Secured	317
Protocol	300	SMP - Socialist	
SECRET - Sprinkling		Millionaire Protocol ...	317
Effect.....	300	SMP-Calling	319
Secret Streams	300	Splitted Secret	319
Secure by Design	301	Spot-On Encryption	
Secure Channel	301	Suite	321
Secure		SQLite	321
Communication	303	StarBeam (Ultra-	
Security	304	StarBeam)	322
Security through		StarBeam-Analyser	322
Obscurity	304	Steganography	322
Selectors	305	Stream Cipher	323
Server	308	Super-Echo	325
Session Management .	308	Surveillance	326
SHA-3	309	Surveillance, global	328
Shared Secret	310	Symmetric Calling	330
Shor's Algorithm	310	Symmetric	
Side-Channel Attack ..	311	Encryption	330
Signal Protocol	312	Symmetric Key	331
Simulacra	313	TCP - Transmission	
SIP-Hash	314	Control Protocol.....	331
Small World		The Ali Baba Cave	331
Phenomenon	314	The Bombe	335
Smoke Aliases for		ThreeFish	336
Key Exchange	316	Timing	337

TLS - Transport Layer Security	337	URN - Uniform Resource Name	354
Token	338	Vapor Protocol	354
Tor	340	Virtual Keyboard	355
Tracking Cookie	340	VEMI - Virtual E-Mail Institution.....	356
Triad of CIA	342	Vigenère Cipher	356
Triple DES	345	Volatile Encryption	359
Trojan Horse	346	Web-of-Trust	359
TEE - Trusted Execution Environment	347	Wide Lanes	360
Turing Machine	348	XKeyscore (Surveillance Program)	360
Turtle-Hopping	350	XMPP - Extensible Messaging and Presence Protocol	361
Twofish	351	XOR	361
Two-Way-Calling	352	YaCy	362
UDP - User Datagram Protocol	352	Zero-Knowledge-Proof	363
URL - Uniform Resource Locator	353		
URL-Distiller	353		
RnD-Questions	364		
Index of Figures	368		
Bibliography	372		
Index of Keywords	397		