

ACRONYMS

3GPP	Third-Generation Partnership Project
5G	Fifth Generation
AES	Advanced Encryption Standard
API	Application Programming Interface
BSGS	Baby Step Giant Step
CA	Certificate Authority
CCA	Chosen Ciphertext Attack
CT	Cipher text
DES	Data Encryption Standard
DH	Diffie- Hellman
DLP	Discrete Logarithmic Problem
DoS	Denial of Service
DSN	Data Sequence Number
DSS	Data Sequence Signal
ECC	Elliptic Curve Cryptography
ECDHP	Elliptic Curve Diffie-Hellman Protocol
ECDLP	Elliptic Curve Discrete Logarithmic Problem
GSM	Global System for Mobile Communication
GSN	Global Sequence Numbers
HMAC	Hash Message Authentication Code
IANA	Internet Assigned Number Authority
IBE	Identity Based Encryption
IDEA	International Data Encryption
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
LIA	Linked Increases Algorithm
LTE	Long-term Evolution
MAC	Message Authentication Code
MD	Message Digest
MitM	Man-in-the-Middle

MPTCP	Multipath Transmission Control Protocol
MPTCPSec	MPTCP Secure
MPTLS	Multipath Transport Layer Security
NAT	Network Address Translation
OLIA	Opportunistic Linked Increases
OS	Operating System
PKG	Private Key Generator
PKI	Public Key Infrastructure
PT	Plaintext
QoS	Quality of Service
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SCMTCP	Secure Connection Multipath TCP
SDN	Software Defined Network
SHA	Secure Hash Algorithm
SKEXMTCP	Secure Key Exchange model for MPTCP
SMKEX	Secure Multipath Key Exchange
SPH	Silver-Pohling-Hellman
SSL	Secure Sockets Layer
SSN	Sub-flow Sequence Number
T/TCP	Transactional Transmission Control Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAV	Unmanned Aerial Vehicle
VM	Virtual Machine
Wi-Fi	Wireless Fidelity
WTCP	Wireless Transmission Control Protocol
wVegas	weighted Vegas