Index

A
active tags 15, 35, 102, 156
Advanced Encryption Standard (AES) 107, 121
Advanced Encryption System (AES) 79
application layer attack 60
Application Level Events (ALE) 20
asymmetric key 2-5, 12, 79
Avoine model 126, 130-131, 135-136

B
back-end server 126, 130, 138-143, 145-148, 152
Backward Link Authentication (BLA) 105
Berlekamp-Massey algorithm 78
binary key tree 193
block ciphers 6, 50, 70-71, 75, 78-79, 82, 94
  modes of operation 79
brand loyalty 180
buffer overflow 52-55, 57, 59-60, 68, 158, 165

c
CARDIS 21, 39-40, 43, 99
CEN (European Committee for Standardization) 16
Certificate Authority (CA) 2
challenge-response procedure 192
Chinese remainder theorem (CRT) 73
Chosen-Ciphertext Attack 197
Chosen-Plaintext Attack 197
ciphertext 2, 6, 9, 37, 78-79, 145
correlation tag 33, 35, 44
cracked tags 44, 140
cracking attack 33-34, 42, 50
close coupling systems 15
counterfeiting 50-52, 140
counterfeiting 50-52, 140
counterfeiting 50-52, 140
cryptology 1, 5-6, 12, 31, 44, 99-100, 121-124, 136-137, 187

cyphertext 2, 6, 9, 37, 78-79, 145
differential power analysis 33, 36-38, 40, 42-44
digital signature 6, 12, 28, 48, 54, 90, 99, 112, 116, 1161, 164, 168-169
direct read 33-35
discrete logarithm problem (DLP) 84, 110
distance-bounding protocol 30-31, 119
distributed DoS (DDoS) 7
Domain Name Server (DNS) 61

E
eavesdropping attacks 25-26, 34, 104, 107, 140
electromagnetic backscatter 15
Electronic Product Code (EPC) 1, 16, 45, 140, 152
  global framework 45, 47
Elgamal encryption 10, 88-89

CRYPTO 30, 36-38, 40, 43-44, 99-100, 121-124

cryptography
lightweight 71, 94, 99, 123
one-way problems 83
toolkit 71, 75
cyclic redundancy check (CRC) 92

D
data
  copying attack 33
  flooding 56
  integrity 39, 46, 48, 113, 164, 168, 187
Data Encryption Standard (DES) 79
decryption key 2, 90
Denial of Service (DoS) 7, 62
differential power analysis 33, 36-38, 40, 42-44
Diffie-Hellman key exchange 3-4, 38
digital signature 6, 12, 28, 48, 54, 90, 99, 112, 116, 161, 164, 168-169
Digital Signature Standard (DSS) 6
direct read 33-35
discrete logarithm problem (DLP) 84, 110
distance-bounding protocol 30-31, 119
Distributed DoS (DDoS) 7
Domain Name Server (DNS) 61

E
eavesdropping attacks 25-26, 34, 104, 107, 140
electromagnetic backscatter 15
Electronic Product Code (EPC) 1, 16, 45, 140, 152
  global framework 45, 47
Elgamal encryption 10, 88-89
Index

Elliptic Curve
   Cryptosystem 11, 40, 42
   encryption 89
encryption key 2, 6, 81, 89
   network architecture 154-156
EPC information service (EPCIS) 155
ETSI (European Telecommunications Standards Institute) 16
Euclidean algorithm (EA) 73
Euler Totient function 72
exhaustive-search protocol 141
extended Euclidean algorithm (EEA) 73

F
Federal Information Processing Standard 3, 98-99
Fermat's little theorem 73
finite field 38, 40, 42, 72-73, 75, 78, 81, 87, 89, 97
flow verification heuristics 176
Forward Link Authentication (FLA) 105
   standards 18

G
general number field sieve (GNFS) algorithm 10
global security 13, 159, 170

H
hardware attacks 33, 39, 42
Hash-based Message Authentication Code (HMAC) 6
hash functions 6, 70-71, 75, 82-83, 92, 94-96, 98-99, 107-108, 113, 118, 121, 141, 193
   lightweight 95
HashLock 192, 205
HB# protocol 114
high-end tags 25, 29
High Frequency (HF) 102
Huffman coding 4, 8

I
information theory 7, 12, 98, 173, 206
integer factorization 9-10, 70-71, 85, 87
   problem 9-10
International Standards Organizations 16
   interrogator 15, 19, 155
Intrusion Detection System (IDS) 7
Intrusion Prevention System (IPS) 7

J
Juels-Weis model 126, 131, 135-136

K
Kerberos protocol 3
Key Distribution Center (KDC) 3
key sharing 2, 4

L
LAST 8, 16, 71, 77, 83, 97, 102, 104, 143, 168, 202, 204-205
Law of Quadratic Reciprocity 74
leaf node 142-143, 193
LibRFID 47
load modulation 15, 29
low-end tags 24
Low Frequency (LF) 102
Low Level Reader Protocol (LLRP) 20, 22

M
malware 48, 53-55, 57-60, 65, 68, 153-175
   back-end 57, 59
Message Authentication Code (MAC) 6, 30, 82, 92, 107
message detection codes (MDC) 92
middleware 18, 20, 22, 45-46, 48, 52-63, 155, 165, 167
   standards 20
mid-range tags 25
Miller-Rabin primality test 75
mimicking 50-51
Molnar-Soppera-Wagner protocol 142-143
Montgomery multiplication algorithm 40

N
National Institute of Standard and Technology (NIST) 6
near-field communications 25
network
   attacks 61
   flow graph 176
notations 141, 196
NP-Complete 177, 183-184, 190
NtruEncrypt 111

O
Object Name Service (ONS) 2
open-source software 46
Optimistic Forward secure RFID Authentication Protocol (O-FRAP) protocol 143
OSK protocol 141-142, 146-147

P
passive tags 15, 19-20, 24, 28, 35, 52, 102, 133, 148, 150
Physically Unclonable Functions (PUF) 186
Pretty Good Privacy (PGP) 4
Privacy Game 197-199, 201-203
proofs 71, 74, 92, 136, 201
public key 2-6, 9-13, 38, 43, 48, 50, 70-73, 85, 87-94, 96-99, 111-112, 122-123, 133-134
Public key infrastructure (PKI) 5, 89

Q
quadratic nonresidue 73

R
reader compromise 179-180, 186
real-time locating 18, 21
Real-time locating systems (RTLS) 21
Refresh Privacy 199-200, 202, 205
relay attack 29-31, 103-105, 115, 117-118, 120
remote-coupling systems 25
replay attack 28-29, 61, 104-105
RFDump 46-47, 54
RFIDIoT 46
RFID (Radio-Frequency IDentification) 1
malware 48, 53, 57, 68, 153-164, 166-171, 173-175
middleware 20, 22, 46, 53-57, 59, 63, 155, 165, 167
privacy 126, 136
standards 14, 16-19, 21, 31, 34, 46, 49, 62, 191
RFscreen 154, 158-161, 164, 166-167, 169-170, 174
architecture 159
threat model 158
RSA Laboratories 9, 50-51
algorithm 10, 38
RSA-OAEP 6
Ryu-Takagi Protocol 145-146, 148

S
Secure Hash Algorithm (SHA-1) 3
Secure Sockets Layer (SSL) 4
security bits 11
session hijacking 28
side channel attack 33, 35-36
simple power analysis 33, 36-38, 40, 42
smartcards 20, 25, 29-31, 49, 161
spoofing 50-52, 63
SQL-injection 158
stream ciphers 75, 78
subtree 142-143
supply chain management 14, 17, 139, 153-155, 158-159, 166, 169-171, 189, 191, 195
model 180, 182, 187
symmetric key 2-5, 11-12, 79, 82, 109, 114

T
attacks on 46
duplication 178-179
flow 176
information leakage 126, 128-129
modification 179, 187
tracking 126, 129, 178, 186
TagEventor 47-48
taint checkpoint 176-177, 184-185, 187
tampering 26-29, 31, 33-35, 39, 43, 92, 104-105, 183
timing analysis 33, 38, 40
memory 103
timing 103
tree-based protocol 142-144, 147
trusted centre (TC) 195
Trusted Third Party (TTP) 3, 7, 89
Index

U
Ultra High Frequency (UHF) 15, 102

V
Vaudenay model 126, 133, 135-136
verification algorithm 185
viruses 7, 48, 52-53, 55, 57-58, 60, 65, 171, 173, 175

W
watermarking 27, 32, 39
wireless link threats 24, 31, 61
worms 55, 57, 59, 65, 68, 175

X
XTR-DSA 114

Y
YA-TRAP 201-204, 207