INDEX

Numbers

2001: A Space Odyssey, 142
2D graphics, 61–69
3D graphics, 69. See also rendering

A

acquire operation, 168, 170
adder circuit, 164
additive color mixing, 60
AES (Advanced Encryption Standard), 9–18, 55
block chaining, 15, 55
combining with RSA, 48–49
data organization under, 11
key expansion, 13–14
overview, 12
performance vs. RSA, 48
possible weaknesses, 17–18
S-box, 13, 14
security of, 16
aliasing, 66, 80, 99
all-pairs shortest path, 183. See also Floyd’s algorithm
alpha blending, 67–68, 82
alpha channel, 68, 78, 82
alpha level, 67
ambient lighting, 96–97
ambient occlusion, 96
American Standard Code for Information Interchange (ASCII), 12, 20–22, 119–120
ASCII (American Standard Code for Information Interchange), 12, 20–22, 119–120
atomic operation, 169
attacks, 2
brute-force, 5, 16, 20, 47
collision, 26
dictionary, 28
frequency analysis, 6, 9, 15, 17
known-plaintext, 6
man-in-the-middle, 52, 56
related-key, 17
timing, 17
authentication, 19, 26, 34. See also RSA
authority, 51, 53
avalanche, 17, 21
Avatar, 69
axis, 61

B

best-first search, 178–181
marked points, 178, 179, 180
reusing results, 181–182
surplus information, 181
B-frame, 139
bidirectional frame, 139
bilinear filtering, 101
in FXAA, 112
binary, 10
ASCII, 12
bit, 10
byte, 10
search, 151
binary addition, 22
binary search, 151–152, 153
binary semaphore, 168
bit, 10
bitmap, 61, 116
alpha channel, 68, 78, 82
coordinate, 61
depth buffer, 91, 95, 96
display buffer, 61
height map, 106
real-time, 108–113
supersampling, 109

How Software Works
© 2015 by V. Anton Spraul
bitmap (continued)
  mipmap, 102
  origin, 61
  resolution, 61
  shadow map, 95
  texture, 97
  translucency, 68, 78

bitwise operations, 11
  AND, 23, 25
  binary addition, 22
  NOT, 23, 25
  OR, 23, 25
  rotation, 14
  XOR, 11, 14, 15

bitwise rotation, 14

Blair Witch Project, The, 142

block chaining, 15

blue difference (Cb), 124

Blu-ray, 116, 143

brute force attack, 5, 16, 20, 47

buffer, shared, 163

buffering, 143

bump mapping, 106, 107

byte, 10

C

Cb (blue difference), 124

cel animation, 59

central processing unit. See CPU
  (central processing unit)
certificate, 53

CGI (computer-generated imagery), 57–59, 82–83. See also
  3D graphics; rendering

chain merging, 31
cipher key. See key (encryption)
ciphertext, 2, 3, 8
circular wait, 172
clear reflection, 103

client, 52

Cloverfield, 142
code book, 9

coefficient, 126

collision, 20, 26

collision attack, 26

color
  additive, 60
  RGB, 60, 116, 124
  subtractive, 60, 76
  YCbCr, 124

composite number, 40

compression, 116

deflate, 122

dictionary, 118–122

Huffman encoding, 120, 134

of JPEG pixel blocks, 132

lossless, 116

lossy, 116, 124

MPEG-2, 138

predictive encoding, 122

quantization, 123, 132

run-length encoding, 117, 123, 133, 142

sliding window, 122

temporal, 138

TGA file format, 122

.com file format, 122

compression ratio, 118

dictionary compression, 120

JPEG, 135

MPEG-4, 143

TGA, 118

.com file, 122

computer security. See security

computer vision, 160

computer-generated imagery (CGI), 57–59, 82–83. See also
  3D graphics; rendering

concurrency, 161

  atomic operation, 169

  deadlock, 172

  multitasking, 162–163, 174

  multiuser environments, 162

  performance, 162

  print spooling, 162

  problems of, 163–166

  race condition, 165–169

  read-only data, 166, 173

  semaphore, 168–174

  shared buffer, 163

  starvation, 170, 172, 173

  transaction, 166–167

control point, 62

coordinates, 61

  axis, 61

  control point, 62

  conversion, 61, 71, 88, 96

  interpolation, 63

  local, 62

  model, 62

  origin, 61

  projection, 71

  scaling, 64

  screen, 61, 88, 96

  translation, 64

  world, 70, 88

  x, 61

  y, 61

  z, 69
coprime number, 40
core, 86, 162, 174
cost, 175, 178, 183, 184
   computing route cost, 179, 182
defining per problem, 175
CPU (central processing unit), 86
   adder, 164
core, 86, 162, 174
   performance characteristics, 86
test-and-set, 169
   updating data, 163, 165
Cr (red difference), 124
crack, 17
crib, 6, 9, 16
cut scene, 86

D
   data collection, 146
      dynamic, 154
      static, 154
   data compression. See compression
   DCT (discrete cosine transform), 125–131, 141
deadlock, 172
deblocking filter, 143
decimal, 10
decryption, 2
deep web, 157
deflate, 122
depth buffer, 91, 95, 96
depth buffering, 91–92
dictionary, 28
dictionary attack, 28
dictionary compression, 118–122
diffuse reflection, 74, 77, 92, 93, 107
diffusion, 16
digital composition, 82
digital image, 59
digital signature, 25–26, 53
      validation, 53
      weaknesses, 26
direct lighting, 76
directed graph, 176
      converting to table, 176
      edge, 176
      point, 176
discrete cosine transform (DCT), 125–131, 141
display buffer, 61
dissolve, 82
distance effect, 72–73, 92
distant impostor, 106, 108
dynamic data collection, 154

E
   edge, 176
   encryption, 2
      avalanche, 17
      crack, 17
      diffusion, 16
      key. See key (encryption)
      one-time pad, 9
      public-key, 38
      RSA. See RSA
      shared key problem, 18, 37
      substitution, 6
      symmetric key, 18
      transposition, 2
   environment mapping, 103–105
   exclusive-or. See XOR

F
   factor, 40, 41
   fast approximate anti-aliasing (FXAA), 111
   field of view, 89
   finding the shortest path, 175
   fixed-size storage, 152, 153
   Floyd’s algorithm, 183–189
      connecting routes, 183, 187
      grid, 183, 186
      improving routes, 185
      route directions, 186–189
   focus, 79
   fps (frames per second), 59, 116, 144
   frame, 59, 116
      buffering, 143
      macroblock, 139
   frame rate, 59
   frames per second (fps), 59, 116, 144
   frequency analysis, 6, 9, 15, 17
   full-screen anti-aliasing, 80
   functions, 39
      hash, 20–21
      invertible, 39–42
      one-way, 39, 42
      square, 39
      square root, 39
      trapdoor, 40
   FXAA (fast approximate anti-aliasing), 111

G
   geographic information systems (GIS), 189
   global illumination model, 76
GPU (graphics processing unit), 87, 90
granularity, 173
graph, directed. See directed graph
graphics accelerator, 86
graphics processing unit (GPU), 87, 90
group of pictures, 138

H
H.264 standard, 143
handshaking, 52–54
hash chaining, 29–31
chain merging, 31
reduction function, 29, 31
hash table, 29, 31
hashing, 20–23, 154–156
avalanche, 17, 21
collision, 20, 26
desirable properties, 20–21
digital signature. See digital signature
encoded password, 21
irreversibility, 20, 25
iterative, 32–33
keyed, 55
MAC, 55
MD5. See MD5
reduction function, 29, 31
rehashing, 156
salt, 34, 35
slot, 154
tombstone, 156
height map, 106
HTTPS, 52–56
authority, 53
certificate, 53
handshaking, 52–54
issuer, 53
MAC, 55
master secret, 54
premaster secret, 53
security of, 55–56
session, 52
transmission, 54–56
Huffman encoding, 120, 142
code creation, 120
in JPEG, 134

I
IDCT (inverse discrete cosine transform), 127
I-frame, 138, 139
images
digital, 51–60
searching for, 160
inbound link, 158
indexing, 152–154
indirect lighting, 76
ink and paint, 59, 65
interpolation, 63
intracoded frame, 138
inverse discrete cosine transform (IDCT), 127
issuer, 53
iterative hashing, 32–33

J
jaggies, 66, 80, 89, 109, 112
Joint Photography Experts Group, 123
JPEG, 123–136
adjusting quality, 135
compressing pixel blocks, 132
compression ratio, 135
DCT, 125
picture quality, 135–136
Jurassic Park, 57–58

K
Kerckhoff’s principle, 4, 5, 27, 33
key (encryption), 4
AES, 9–14
asymmetric, 38
code book, 9
expansion, 9
keyed hashing, 55
MAC, 55
private, 38, 44, 45, 50
public, 38, 43, 44, 45, 50
related-key attack, 17
shared key problem, 18, 37
size, 20, 47
symmetric, 18
key (search), 146, 151
key expansion, 9
keyframe, 59
known-plaintext attack, 6

L
Lady and the Tramp, 59
LaserDisc, 116
LCD (liquid crystal display), 60
light-emitting diode (LED), 60
lighting, 71–80
ambient, 96–97
angle of incidence, 74, 75
angle of reflectance, 74
bump mapping, 106, 107
diffuse reflection, 74, 77, 92, 93, 107
direct, 76
distance effect, 72–73, 92
indirect, 76
model, 72
normal, 92, 93, 107
ray tracing. See ray tracing
real-time, 92–97
reflection, 80
clear, 103
environment mapping, 103–105
shadow. See shadow
specular reflection, 75, 77, 92, 107
link farming, 159
links
farming, 159
inbound, 158
pass-through, 159
liquid-crystal display (LCD), 60
local coordinate, 62
lossless compression, 116
lossy compression, 116, 124
luminance, 124

M
MAC, 55
macroblock, 139
deblocking filter, 143
man-in-the-middle attack, 52, 56
map
converting to table, 176
directed graph, 176
routing. See routing
massively multiplayer online game (MMO), 164
master secret, 54
matrix, 128
matrix multiplication, 126
MD5, 21–25
digital signature, 25–26
encoding password for, 21–22
quality of, 25
round, 24–25
message authentication code, 55
mipmap, 102
MMO (massively multiplayer online game), 164
model, 61–63, 70, 87
ambient light, 96
bump mapping, 106
control point, 62
distant impostor, 106
drawing, transforming into, 62, 88, 93, 105
global illumination, 76
interpolation, 63
lighting, 72
line, 62
scaling, 64
tessellation, 107–108
translation, 64
Mortal Kombat, 85
movie-quality rendering, 70, 82–83
MPEG-2, 138–142
adjusting quality, 139
B-frame, 139
GOP, 138, 142
I-frame, 138, 139
macroblock, 139
P-frame, 139
MPEG-4, 143
multisample anti-aliasing (MSAA), 110–111
vs. supersampling, 111
multitasking, 162–163, 174

N
nearest-neighbor sampling, 99–100, 101, 143
normal, 92, 93, 107
NOT (bitwise operation), 23, 25
numerical address, 153

O
offset, 139
one-time pad, 9
one-way function, 39, 42
optical printer, 82
OR (bitwise operation), 23, 25
origin, 61

P
packet, 118
painter’s algorithm, 90
partition, 147
pass-through link, 159
password, 6, 19
common, 28, 29
encoding, 21–22
hashing, 20–23
salt, 34, 35
storage service, 35–36
table, 26, 27
performance scaling, 150
persistence of vision, 59
P-frame, 139
Phineas and Ferb, 69
pivot, 147
pixel, 59, 66
  alpha channel, 68
  alpha level, 67, 78, 82
  bitmap, 61
  contrast, 112
  depth, 91, 95, 96
  luminance, 124
  raw, 117
  run, 117
  sampling, 97
  shader, 92. See also lighting
  subpixel, 110
  texel, 98
  variation in photographs, 123
plaintext, 2, 3, 4, 8, 27, 28
  known-plaintext attack, 6
polyalphabetic substitution, 7–9
polygon, 88. See also triangle
post-process anti-aliasing, 111
precomputed hash table, 29, 31
predicted frame, 139
predictive encoding, 122
prefix code, 121
premaster secret, 53
prime number, 40
  as factor, 41
  coprime, 40
prime-product, 42, 44, 45
print spooling, 162
private key, 38, 44, 45, 50
process, 162
projection, 71, 88, 96
  field of view, 89
  ray tracing, 77
public key, 38, 43, 44, 45, 50
quantization, 123, 132, 141
queue, 163, 170
quicksort, 147–150
  partition, 147
  pivot, 147
  sublist, 149
race condition, 165–169
rasterization, 65–68, 89
raw pixel, 117
ray tracing, 77–81, 105
  anti-aliasing, 80
  focus, 79
laws of optics, 79
performance, 87
projection, 77
reflection, 80
shadow, 79
read semaphore, 173
read-only data, 166, 173
real-time lighting, 92–97
record, 146
red difference (Cr), 124
reduction function, 29, 31
  clear, 103
  environment mapping, 103–105
rehashing, 156
related-key attack, 17
release operation, 168
renderer, 69
rendering, 69
  2D, 61–69
    budget, 113
    depth buffering, 91–92
    depth ordering, 89–92
    field of view, 89
    focus, 79
    lighting, 71–80
    movie-quality, 70, 82–83
    pixel shader, 92
    polygon, 88
    projection, 71
    rasterization, 89
    ray tracing, 77–81
    realism, 72, 79, 94, 96, 105
    reflection, 80
    translucency, 78
    triangle, 88, 90
    viewpoint, 71
resolution, 61
RGB color system, 60, 124
  vs. YCbCr, 124
Rivest, Shamir, and Adleman method.
  See RSA (Rivest, Shamir, and
  Adleman method)
robot, 157, 160
rotation, 14
routing
  cost, 175, 178, 179, 182, 183, 184
  directed graph, 176
  finding the shortest path, 175
  using real-time data, 189
RSA (Rivest, Shamir, and Adleman
  method), 42–51
  authentication, 49–51
  authority, 51
How Software Works
© 2015 by V. Anton Spraul
bidirectional transmission, 47
combining with AES, 48–49
effectiveness, 45–47
encryption process, 44–45
key creation, 42–44
key size, 47
performance, 47–48
prime-product, 42, 44, 45
real-world use, 47–49
totient, 43, 45
run of pixels, 117
run-length encoding, 117, 123, 133, 142

S
salt method, 34, 35
sampling, 97
  bilinear filtering, 101, 112
  mipmap, 102
  nearest-neighbor, 99–100, 101, 143
  trilinear filtering, 102–103
S-box, 13, 14
scaling, 64, 150
screen coordinate, 61, 88, 96
screen space ambient occlusion (SSAO), 96–97
search, 29, 145
  all-pairs shortest path, 183
  best-first, 178–181
  binary, 151–152, 153
  engine, 157
  images, 160
  location use, 160
  page ranking, 158–159
  robot, 157, 160
  sequential, 146, 153
  Sitemap, 157
  storage requirements, 153
  term, 159–160
  Web, 157–160
security, 1, 17, 19, 35
  of AES, 16
  best practices, 6, 27, 29, 34, 56
  single point of defense, 27
  Web, 52–56
selection sort, 146
  performance scaling, 150
semaphore, 168–174
  acquire, 168, 170
  binary, 168
  circular wait, 172
  granularity, 173
  implementation, 169
  performance, 172–174
read, 173
release, 168
spin lock, 169
test-and-set, 169
wait list, 170
write, 173
sequential search, 146, 153
server, 52
session, 52
shadow, 79, 94–97
  ambient occlusion, 96
  mapping, 94–95
  quality, 95
shadow map, 95
shared buffer, 163
shared key problem, 18, 37
signature. See digital signature
simple substitution, 6
Simpsons, The, 69
single point of defense, 27
Sitemap, 157
sliding window, 122
slot, 154
sort, 146
  quicksort, 147
  selection sort, 146
specular reflection, 75, 77, 92, 107
spin lock, 169
square function, 39
square root function, 39
SSAA (supersampling anti-aliasing), 109–110
  vs. multisampling, 111
SSAO (screen space ambient occlusion), 96–97
starting variable, 15
starvation, 170, 172, 173
static data collection, 154
storage
  address, 153
  fixed-size, 152, 153
  requirements for search, 153
  variable-size, 152, 153
subpixel, 110
substitution, 6–9
  polyalphabetic, 7
  S-box, 13
  simple, 6
  tabula recta, 7
subtractive color mixing, 60, 76
supersampling anti-aliasing (SSAA), 109–110
  vs. multisampling, 111
surface normal. See normal
symmetric key, 18
tabula recta, 7
temporal compression, 138
temporal redundancy, 138, 142
tessellation, 107–108
test-and-set, 169
texel, 98
texture mapping, 97–103, 143
  bump mapping, 106
  sampling, 97
TGA file format, 117
  compression ratio, 118
  packet, 118
Theora, 143
timing attack, 17
tombstone, 156
Toon Boom, 69
Toonz, 69
totient, 43, 45
transaction, 164, 166–167
translation, 64
translucency, 68, 78
transposition, 2–6
  rotation, 14
trapdoor function, 40
triangle, 88, 90, 107
trilinear filtering, 102–103, 143
trivial factor, 40
tweening, 59
  automatic, 63–64
ultra high definition video (UHD), 144
variable-size storage, 152, 153
vector, 126
video streaming, 116
videocassette, 115
view angle, 74
viewpoint, 71
virtual camera, 71
War and Peace, 122
web search, 157–160
web session, 52
world coordinate, 70, 88
write semaphore, 173
x-axis, 61
x-coordinate, 61
XOR (bitwise operation), 11, 14, 15
y-axis, 61
YCbCr color system, 124
  vs. RGB, 124
y-coordinate, 61
Y (luminance), 124
z-coordinate, 69
.zip file format, 122