

Sommario

RINGRAZIAMENTI	XI
INTRODUZIONE	XIII
A chi è dedicato questo libro	XIII
Argomenti trattati	XIV
Dietro le quinte della magia	XV
CRITTOGRAFIA	1
Lo scopo della crittografia	2
La trasposizione: stessi dati, ordine differente	2
Chiavi di cifratura	4
Attaccare la cifratura	6
Sostituzione: rimpiazzare i dati	7
Variare lo schema di sostituzione	8
Espansione della chiave	10
L'Advanced Encryption Standard	11
Basi di matematica binaria	11
Cifratura AES: una visione d'insieme	14
L'espansione delle chiavi nell'AES	15
Passaggi di cifratura AES	16
Perché l'AES è sicuro	19
Possibili attacchi all'AES	20
I limiti della crittografia a chiave privata	21
PASSWORD	23
Trasformare una password in un numero	23
Proprietà di una buona funzione hash	24
La funzione hash MD5	25
Codifica della password	25
Operazioni bit a bit	26
Fasi della funzione MD5	28
Soddisfare i requisiti di una buona funzione hash	29

Firme digitali	30
Il problema dell'identità	30
Attacco tramite collisioni	31
Le password nei sistemi di autenticazione	31
Pericoli insiti nelle tabelle di password	32
Effettuare l'hashing delle password	33
Attacchi a dizionario	34
Tabelle hash	35
Concatenazione hash	35
Hashing iterativo	38
"Salare" le password	40
Le tabelle delle password sono sicure?	41
Sistemi di archiviazione delle password	41
Considerazioni finali	42
SICUREZZA E WEB	43
La crittografia a chiave pubblica risolve il problema della chiave condivisa	43
Strumenti matematici per la crittografia a chiave pubblica	44
Funzioni invertibili	45
Funzioni unidirezionali	45
Funzioni trapdoor	46
Il metodo di cifratura RSA	48
Creazione delle chiavi	49
Cifrare dati con l'RSA	51
L'efficacia dell'RSA	51
L'uso dell'RSA nella pratica	54
RSA per l'autenticazione	57
Sicurezza nel web: l'HTTPS	59
Handshaking	60
La trasmissione dei dati nell'HTTPS	62
Il problema della chiave condivisa è risolto?	63
COMPUTER GRAFICA E CINEMA	65
Software per l'animazione tradizionale	67
Come funzionano le immagini digitali	67

Definizione dei colori	69
Come il software crea le animazioni	70
Dal software per le animazioni alla grafica 2D renderizzata	77
Software per la CGI in 3D	78
Come vengono descritte le scene 3D	79
La macchina da presa virtuale	80
Illuminazione diretta	81
Illuminazione globale	85
Il tracciamento della luce	86
Anti-aliasing dell'intera scena	90
Combinare il reale e l'artificiale	91
Il rendering di qualità cinematografica ideale	92
TECNOLOGIE GRAFICHE PER I VIDEOGIOCHI	95
Hardware per grafica in tempo reale	96
Perché nei videogiochi non si usa il ray tracing	97
Solo rette, niente curve	98
Proiezione in assenza di ray tracing	98
Rendering dei triangoli	100
L'algoritmo del pittore	101
Depth buffering	101
Illuminazione in tempo reale	103
Ombre	105
Illuminazione e occlusione ambientale	107
Texture mapping	109
Campionamento nearest-neighbour	111
Filtraggio bilineare	113
Mipmap	114
Filtraggio trilineare	115
Riflessioni	116
Imitare le curve	119
Distant impostors	119
Bump mapping	120
Tassellazione	121

Anti-aliasing in tempo reale	122
Sovracampionamento	123
Multicampionamento	125
Anti-aliasing post-processo	125
Il budget per il rendering	127
Qual è il futuro della grafica per videogiochi?	128
COMPRESSIONE DATI	131
Codifica run-length	133
Compressione a dizionario	135
Funzionamento	135
Codifica Huffman	136
Riorganizzare i dati per una compressione migliore	138
Codifica predittiva	138
Quantizzazione	139
Immagini JPEG	140
Un modo diverso di registrare i colori	141
La trasformata discreta del coseno	142
La DCT in due dimensioni	146
Comprimere i risultati	150
La qualità delle immagini JPEG	154
Compressione di video in alta definizione	157
Ridondanza temporale	157
Compressione video MPEG-2	158
Qualità video con compressione temporale	162
Presente e futuro della compressione video	163
RICERCA	165
Definire il problema della ricerca	165
Ordinare i dati	166
Ordinamento per selezione	166
Quicksort	167
Ricerca binaria	171
Indicizzazione	172
Hashing	175
Ricerche nel web	178

Creare una classifica dei risultati	179
Usare l'indice in modo efficace	181
Qual è il futuro delle ricerche sul web?	182
CONCORRENZA	185
Perché è necessaria la concorrenza	185
Prestazioni	185
Ambienti multiutente	186
Multitasking	186
La concorrenza può incepparsi	187
Rendere sicura la concorrenza	190
Dati in sola lettura	191
Procedure basate su transazioni	191
Semafori	192
Il problema delle attese indeterminate	194
Code ordinate	195
Starvation causata da attese circolari	195
Semafori e prestazioni	198
Qual è il futuro per la concorrenza	199
MAPPE E ITINERARI	201
Come un software vede una mappa	201
Ricerca best-first	204
Riutilizzo di risultati di ricerche precedenti	207
Trovare tutti i migliori itinerari in un colpo solo	208
L'algoritmo di Floyd	209
Archiviare le indicazioni stradali	212
Il futuro della navigazione	215
INDICE ANALITICO	217