Paolo Ferragina e Fabrizio Luccio

Crittografia

Principi Algoritmi Applicazioni

Bollati Boringhieri

Indice

7 *Prefazione*

Crittografia

11 1. La crittografia: una visione di insieme

1.1 Cifratura, decifrazione, attacchi dall'esterno, 13 1.2. Livelli di segretezza, 16 1.3. La chiave pubblica, 18 1.4. L'approccio algoritmico, 19 1.5. Applicazioni, 20

22 2. Rappresentazione e calcolabilità

2.1. Alfabeti e sequenze, 22 2.2. L'ordinamento canonico, 25 2.3. Funzioni, problemi e algoritmi, 26

30 3. Algoritmi e complessità

3.1. Paradigmi algoritmici, 31 3.2. Complessità computazionale, 37 3.3. Algoritmi polinomiali e esponenziali, 42 3.4. Le classi P, NP, co-NP e NPC, 48

55 4. Il ruolo del caso

4.1. Il significato algoritmico della casualità, 56 4.2. Generatori di numeri pseudo-casuali, 60 4.3. Algoritmi randomizzati, 65

71 5. Cifrari storici

5.1. Il cifrario di Cesare, 72 5.2. Una classificazione dei cifrari storici, 74 5.3. Cifrari a sostituzione monoalfabetica, 75 5.4. Cifrari a sostituzione polialfabetica, 77 5.5. Cifrari a trasposizione, 79 5.6. Crittoanalisi statistica, 82

86 6. Cifrari perfetti

6.1. Il cifrario One-Time Pad, 88 6.2. Generazione della chiave , 91

95 7. Il cifrario simmetrico standard

7.1. Un po' di storia, 96 7.2. Il cifrario *DES*, 97 7.3. Attacchi, variazioni e alternative al *DES*, 104 7.4. Cifrari a composizione di blocchi, 108 7.5. *AES*: il nuovo standard, 110

113 8. Crittografia a chiave pubblica

8.1. Alcuni richiami di algebra modulare, 115 8.2. Le funzioni one-way trap-door, 118 8.3. Pregi e difetti del nuovo metodo, 120 8.4. Il cifrario *RSA*, 121 8.5. Attacchi all'*RSA*, 124 8.6. I cifrari ibridi, 127

130 9. Identificazione, autenticazione e firma digitale

9.1. Funzioni hash one-way, 131 9.2. Identificazione, 133 9.3. Autenticazione, 134 9.4. Firma digitale, 136 9.5. Attacchi al protocollo di firma, 140 9.6. La *Certification Authority*, 142

146 10. Un esempio: il protocollo *SSL*

10.1. Il protocollo *SSL Handshake*, 147 10.2. Sicurezza del protocollo *SSL*, 151

155 *Bibliografia*

159 *Indice analitico*