

Tartalom

<i>Előszó</i>	9
I. rész Kriptográfiai primitívek	13
<i>1. Alapfogalmak</i>	<i>15</i>
1.1. Feltétel nélkül biztonságos rejtjelezés: a One-Time-Pad	19
1.2. Feltétel nélkül biztonságos hitelesítés	21
1.3. Feladatok	22
<i>2. Szimmetrikus kulcsú blokkrejtjelezők</i>	<i>25</i>
2.1. Helyettesítéses-permutációs rejtjelezők és a DES	27
2.2. Helyettesítéses-permutációs rejtjelezők tervezése	32
2.3. Differenciális és lineáris kriptanalízis	52
2.4. Algebrai zártság és többszörös rejtjelezés	68
2.5. Az AES blokkrejtjelező	72
2.6. Feladatok	75
<i>3. Nyilvános (aszimmetrikus) kulcsú rejtjelezők</i>	<i>79</i>
3.1. Az RSA algoritmus	80
3.2. Az RSA biztonsága	83
3.3. Prímszámok keresése	86
3.4. Elliptikus görbe kriptográfia	89
3.5. Feladatok	94
<i>4. Kriptográfiai hash függvények</i>	<i>99</i>
4.1. Hash függvény fajták és biztonsági kritériumok	99
4.2. A születésnap paradoxon	105

6	Tartalom	
	4.3. Bizonyítható biztonságú konstrukciók	106
	4.4. Feladatok	110
	II. rész Kriptográfiai alprotokollok	115
	5. <i>Blokkrejtjelezési módok</i>	<i>117</i>
	5.1. Az ECB mód	118
	5.2. A CBC mód	120
	5.3. A CFB mód	133
	5.4. Az OFB mód	136
	5.5. A CTR mód	139
	5.6. Összefoglalás	140
	5.7. Feladatok	142
	6. <i>Üzenethitelesítés</i>	<i>145</i>
	6.1. A CBC MAC	147
	6.2. Hash függvényre épülő MAC függvények	149
	6.3. Feladatok	154
	7. <i>Digitális aláírás</i>	<i>157</i>
	7.1. Támadások osztályozása	159
	7.2. Lenyomat aláírása (a „hash-and-sign” paradigma)	161
	7.3. Példák digitális aláírásémákra	163
	7.4. Feladatok	165
	8. <i>Kulcscsere protokollok</i>	<i>167</i>
	8.1. Kulcscsere protokollok osztályozásának szempontjai	168
	8.2. Támadó modell	172
	8.3. Példák kulcsszállító protokollokra	174
	8.4. Példák kulcsmegegyezés protokollokra	189
	8.5. Nyilvános kulcs infrastruktúra alapjai	191
	8.6. Informális protokoll-tervezési elvek	199
	8.7. Kulcscsere protokollok formális ellenőrzése és a BAN-logika	205
	8.8. Feladatok	219
	9. <i>Partner-hitelesítés</i>	<i>221</i>
	9.1. Jelszó alapú partner-hitelesítés	222
	9.2. Kihívás-válasz protokollok	226
	9.3. Zero-knowledge-protokollok partner-hitelesítésre	228
	9.4. Feladatok	232

III. rész Alkalmazások	235
<i>10. Internet biztonsági protokollok</i>	<i>237</i>
10.1. SSL (Secure Socket Layer)	237
10.2. IPSec	255
10.3. PGP (Pretty Good Privacy)	261
<i>11. Mobil hálózatok biztonsága</i>	<i>265</i>
11.1. GSM biztonság	266
11.2. UMTS biztonság	271
<i>12. Elektronikus fizetési protokollok</i>	<i>275</i>
12.1. Elektronikus fizetési rendszerek (EPS) csoportosítása	276
12.2. Hitelkártyás fizetés az interneten: SET	278
12.3. Digitális készpénz: DigiCash	284
12.4. Mikrofizetési protokollok: PayWord	288
IV. rész Fejezetek a bizonyítható biztonság elméletéből	293
<i>13. Alapfogalmak</i>	<i>295</i>
13.1. Bonyolultságosztályok, orákulum, redukció	297
13.2. Egyirányú függvény (One Way Function – OWF)	303
13.3. Csapda egyirányú permutáció	306
13.4. Keménybit	312
13.5. Feladatok	318
<i>14. Véletlen és algoritmikus megkülönböztethetőség</i>	<i>321</i>
14.1. Valószínűség-eloszlások algoritmikus megkülönböztethetősége	322
14.2. Polinomiális időben megkülönböztethetőség	325
14.3. Feladatok	328
<i>15. Álvéletlen-generátor</i>	<i>331</i>
15.1. Álvéletlen-generátor és az egyirányú függvény	332
15.2. Álvéletlen-generátor konstrukció	334
15.3. Feladatok	335
<i>16. Álvéletlen függvény, álvéletlen permutáció</i>	<i>339</i>
16.1. Véletlen függvény, álvéletlen függvény	340
16.2. Álvéletlen függvény konstrukció	341

8 Tartalom

16.3. Álvéletlen permutáció konstrukció	344
16.4. PRF alkalmazás példák	349
16.5. Feladatok	349
<i>17. Szimmetrikus kulcsú rejtjelező leképezés modelljei</i>	<i>353</i>
17.1. Véletlen függvénytől megkülönböztetés	354
17.2. Kulcsfejtés elleni biztonság	359
17.3. Nyílt szöveg visszafejtő támadás	362
17.4. Üzenet-megkülönböztető támadás	363
<i>18. Biztonságos nyilvános kulcsú rejtjelezés</i>	<i>371</i>
18.1. Szemantikai biztonság	372
18.2. Üzenet-megkülönböztethetetlenség biztonság	374
18.3. Rejtjeles szöveg módosíthatatlanság biztonság	388
18.4. Feladatok	392
<i>19. A véletlen orákulum bizonyítástechnika</i>	<i>393</i>
19.1. <i>ind</i> – <i>cpa</i> -biztonság véletlen orákulum modellben	395
<i>20. Biztonságos digitális aláírás</i>	<i>399</i>
20.1. Biztonságos one-time aláírás	400
20.2. Aláírás az RSA algoritmus felhasználásával	401
<i>21. Üzenethitelesítés (MAC) biztonsága</i>	<i>405</i>
<i>A kitűzött feladatok megoldása</i>	<i>409</i>
Függelékek	439
<i>A – Kapcsolódó szabványok</i>	<i>439</i>
<i>Irodalom</i>	<i>443</i>