



# Índex

I	Conceptes bàsics	
<b>1</b>	<b>Introducció a la criptografia</b>	<b>13</b>
1.1	Conceptes bàsics	13
1.1.1	Introducció a la criptoanàlisi	16
1.2	Una mica d'història	17
1.2.1	Xifres de transposició	19
1.2.2	Xifres de substitució	20
1.3	Resum	27
1.4	Solucions dels exercicis	28
1.5	Bibliografia	30
<b>2</b>	<b>Fonaments matemàtics</b>	<b>31</b>
2.1	Aritmètica modular	32
2.1.1	Estructures algebraiques: grups, anells i cossos	32
2.1.2	Divisibilitat als enters	34
2.1.3	Aritmètica modular amb enters	37
2.1.4	Aritmètica modular amb polinomis	45
2.2	Nombres primers	48
2.2.1	Tests de primalitat	49
2.3	Problemes matemàtics difícils	52
2.3.1	Complexitat d'un algorisme	52
2.3.2	Producte de primers i factorització d'enters	53
2.3.3	Exponenciació i logaritme discret	54
2.3.4	Quadrats i arrels quadrades modulars	54

<b>2.4</b>	<b>Resum</b>	<b>55</b>
<b>2.5</b>	<b>Solucions dels exercicis</b>	<b>56</b>
<b>2.6</b>	<b>Bibliografia</b>	<b>58</b>

## II

## Criptografia de clau simètrica

<b>3</b>	<b>Les xifres de flux</b>	<b>61</b>
<b>3.1</b>	<b>Criptografia de clau simètrica o compartida</b>	<b>62</b>
<b>3.2</b>	<b>Definició de les xifres de flux</b>	<b>62</b>
3.2.1	Període	64
3.2.2	Aleatorietat	64
<b>3.3</b>	<b>Generadors lineals de seqüència xifrant</b>	<b>69</b>
3.3.1	Generadors congruencials	69
3.3.2	Registres de desplaçament reallimentats linealment (LFSR)	69
3.3.3	Limitacions dels generadors lineals	73
<b>3.4</b>	<b>Generadors no lineals</b>	<b>74</b>
3.4.1	A5	75
3.4.2	Trivium	78
<b>3.5</b>	<b>Resum</b>	<b>82</b>
<b>3.6</b>	<b>Solucions dels exercicis</b>	<b>83</b>
<b>3.7</b>	<b>Bibliografia</b>	<b>84</b>
<b>4</b>	<b>Les xifres de bloc</b>	<b>85</b>
<b>4.1</b>	<b>Definició de les xifres de bloc</b>	<b>85</b>
4.1.1	Modes d'operació	86
<b>4.2</b>	<b>El criptosistema AES</b>	<b>91</b>
4.2.1	Descripció del funcionament	92
4.2.2	Detall d'una iteració	94
4.2.3	Funció AddRoundKey	94
4.2.4	Funció ByteSub	95
4.2.5	Funció ShiftRow	96
4.2.6	Funció MixColumns	97
4.2.7	Generació de subclaus	98
4.2.8	Desxifrat	101
<b>4.3</b>	<b>Resum</b>	<b>102</b>
<b>4.4</b>	<b>Solucions dels exercicis</b>	<b>103</b>
<b>4.5</b>	<b>Bibliografia</b>	<b>107</b>
<b>5</b>	<b>Funcions hash</b>	<b>109</b>
<b>5.1</b>	<b>Les funcions hash</b>	<b>109</b>
5.1.1	Definicions	110
5.1.2	Propietats	111
5.1.3	Seguretat de les funcions hash	112

<b>5.2</b>	<b>Construcció de funcions hash</b>	<b>113</b>
5.2.1	Funcions hash basades en criptosistemes de bloc	114
5.2.2	Funcions hash de disseny específic	116
<b>5.3</b>	<b>L'estàndard SHA-256</b>	<b>117</b>
5.3.1	Padding del missatge	117
5.3.2	Funció de compressió del SHA-256	118
5.3.3	SHA-256 sobre múltiples blocs	124
<b>5.4</b>	<b>Aplicacions de les funcions hash</b>	<b>124</b>
5.4.1	Codis d'autenticació de missatges	125
5.4.2	Resum de missatges	127
5.4.3	Emmagatzematge de contrasenyes	127
5.4.4	Derivació de claus	129
5.4.5	Pseudonimització de dades	130
5.4.6	Generació de cadenes de bits pseudoaleatòries	132
5.4.7	Compromís de bit	132
5.4.8	Prova de treball	134
5.4.9	Taules hash	135
5.4.10	Arbres de Merkle	138
5.4.11	Filtres de Bloom	141
<b>5.5</b>	<b>Funcions hash amb propietats addicionals</b>	<b>149</b>
<b>5.6</b>	<b>Resum</b>	<b>151</b>
<b>5.7</b>	<b>Solucions dels exercicis</b>	<b>152</b>
<b>5.8</b>	<b>Bibliografia</b>	<b>156</b>



## Criptografia de clau pública

<b>6</b>	<b>Criptografia de clau pública</b>	<b>159</b>
<b>6.1</b>	<b>L'origen de la criptografia de clau pública</b>	<b>159</b>
<b>6.2</b>	<b>Intercanvi de claus de Diffie-Hellman</b>	<b>161</b>
<b>6.3</b>	<b>Xifres de clau pública</b>	<b>163</b>
6.3.1	Xifratge basat en la factorització d'enters: RSA	163
6.3.2	Xifratge basat en el logaritme discret: ElGamal	166
<b>6.4</b>	<b>Signatures digitals</b>	<b>168</b>
6.4.1	Signatures basades en la factorització d'enters: RSA	169
6.4.2	Signatures basades en el logaritme discret: ElGamal	170
6.4.3	Atacs als esquemes de signatura digital	173
<b>6.5</b>	<b>Criptografia simètrica i asimètrica</b>	<b>175</b>
<b>6.6</b>	<b>Implementació dels algorismes de clau pública</b>	<b>177</b>
6.6.1	Optimització del xifrat RSA	177
6.6.2	Optimització del desxifrat RSA	178
6.6.3	Optimització del xifrat ElGamal	180
6.6.4	Optimització del desxifrat ElGamal	180

<b>6.7</b>	<b>Criptografia post-quàntica</b>	<b>180</b>
<b>6.8</b>	<b>Resum</b>	<b>182</b>
<b>6.9</b>	<b>Solucions dels exercicis</b>	<b>183</b>
<b>6.10</b>	<b>Bibliografia</b>	<b>185</b>
<b>7</b>	<b>Infraestructura de clau pública</b>	<b>187</b>
<b>7.1</b>	<b>Entitats d'una PKI</b>	<b>187</b>
7.1.1	Autoritat de certificació	188
7.1.2	Autoritat de registre	189
7.1.3	Autoritat de validació	189
7.1.4	Autoritat de segellat de temps	190
7.1.5	Entitat final	190
7.1.6	Repositori de certificats	191
7.1.7	Repositori de llistes de revocació de certificats	191
<b>7.2</b>	<b>Cicle de vida d'un certificat digital</b>	<b>191</b>
7.2.1	Generació del parell de claus	191
7.2.2	Registre	193
7.2.3	Creació del certificat	193
7.2.4	Disseminació i recuperació del certificat	194
7.2.5	Validació del certificat	194
7.2.6	Expiració del certificat	195
7.2.7	Revocació del certificat	195
7.2.8	Història i arxivament de claus	195
<b>7.3</b>	<b>Els estàndards X.509</b>	<b>196</b>
7.3.1	Certificats de clau pública	196
7.3.2	Llistes de revocació de certificats	201
7.3.3	Online Certificate Status Protocol	206
7.3.4	Time Stamp Protocol	206
7.3.5	Estructures de PKI	208
<b>7.4</b>	<b>Les normes PKCS</b>	<b>209</b>
7.4.1	PKCS#1	210
7.4.2	PKCS#5	217
7.4.3	PKCS#12	218
<b>7.5</b>	<b>Formats de representació de dades</b>	<b>218</b>
<b>7.6</b>	<b>Els problemes de la PKI en desplegaments reals</b>	<b>220</b>
<b>7.7</b>	<b>Resum</b>	<b>223</b>
<b>7.8</b>	<b>Solucions dels exercicis</b>	<b>224</b>
<b>7.9</b>	<b>Bibliografia</b>	<b>225</b>
<b>8</b>	<b>Criptografia de corbes el·líptiques</b>	<b>227</b>
<b>8.1</b>	<b>L'origen de la criptografia de corbes el·líptiques</b>	<b>227</b>
<b>8.2</b>	<b>Beneficis de la criptografia de corbes el·líptiques</b>	<b>229</b>
<b>8.3</b>	<b>Corbes el·líptiques</b>	<b>230</b>
8.3.1	Corbes el·líptiques sobre els reals	231
8.3.2	Corbes el·líptiques sobre cossos finits	235

<b>8.4</b>	<b>Corbes el·líptiques per a usos criptogràfics</b>	<b>243</b>
8.4.1	Selecció verificablement pseudoaleatòria de corbes	244
8.4.2	Corbes estandarditzades	246
8.4.3	Funcions hash que retornen punts de corbes el·líptiques	250
<b>8.5</b>	<b>El problema del logaritme discret sobre corbes el·líptiques</b>	<b>251</b>
<b>8.6</b>	<b>Criptografia basada en el problema del logaritme discret sobre corbes</b>	<b>252</b>
8.6.1	Intercanvi de claus de Diffie-Hellman amb corbes el·líptiques	252
8.6.2	L'esquema de signatura ECDSA	253
8.6.3	L'esquema de xifratge integrat de corbes el·líptiques (ECIES)	256
<b>8.7</b>	<b>Resum</b>	<b>258</b>
<b>8.8</b>	<b>Solucions dels exercicis</b>	<b>259</b>
<b>8.9</b>	<b>Bibliografia</b>	<b>263</b>
<b>9</b>	<b>Criptografia basada en pairings</b>	<b>265</b>
<b>9.1</b>	<b>Propietats dels pairings</b>	<b>265</b>
<b>9.2</b>	<b>Eines matemàtiques per a la construcció dels pairings</b>	<b>266</b>
9.2.1	Corbes el·líptiques sobre cossos estesos	266
9.2.2	Els punts de la $r$ -torsió	267
9.2.3	El divisor d'una funció	268
9.2.4	Construcció de funcions a partir del divisor	275
<b>9.3</b>	<b>Construcció explícita dels pairings de Weil i Tate</b>	<b>277</b>
9.3.1	El <i>pairing</i> de Weil	277
9.3.2	El <i>pairing</i> de Tate	280
<b>9.4</b>	<b>Algorismes criptogràfics basats en pairings</b>	<b>281</b>
9.4.1	L'esquema de signatura BLS	282
9.4.2	Criptografia basada en la identitat	287
<b>9.5</b>	<b>Resum</b>	<b>291</b>
<b>9.6</b>	<b>Solucions dels exercicis</b>	<b>292</b>
<b>9.7</b>	<b>Bibliografia</b>	<b>294</b>

## IV

## Protocols criptogràfics

<b>10</b>	<b>Protocols criptogràfics</b>	<b>297</b>
<b>10.1</b>	<b>El protocol de tres passos de Shamir</b>	<b>297</b>
10.1.1	El xifrat de Vernam i el protocol de tres passos de Shamir	298
10.1.2	El criptosistema d'exponenciació	299
<b>10.2</b>	<b>Esquemes de compartició de secrets</b>	<b>300</b>
10.2.1	Esquema de compartició de secrets polinòmic	300
10.2.2	Problemàtiques dels esquemes de compartició de secrets	302
<b>10.3</b>	<b>Esquemes de compromís de bit</b>	<b>303</b>
10.3.1	Compromís de bit utilitzant funcions hash	304
10.3.2	Compromís de Pedersen	304
10.3.3	Aplicacions dels esquemes de compromís de bit	305

<b>10.4</b>	<b>Signatures cegues</b>	<b>306</b>
10.4.1	Signatura cega amb RSA	306
10.4.2	Aplicacions de les signatures cegues	307
10.4.3	Protecció contra abusos en les signatures cegues	308
<b>10.5</b>	<b>Signatures d'anell</b>	<b>309</b>
10.5.1	Les signatures d'anell basades en RSA	310
<b>10.6</b>	<b>Proves de coneixement nul</b>	<b>316</b>
10.6.1	Prova del coneixement del logaritme discret	318
10.6.2	Aplicacions de les proves de coneixement nul	319
<b>10.7</b>	<b>Protocol de transferència inconscient</b>	<b>319</b>
10.7.1	Protocol d'Even, Goldreich i Lempel	320
10.7.2	Aplicacions de la transferència inconscient	321
<b>10.8</b>	<b>Protocols de recuperació privada d'informació</b>	<b>322</b>
10.8.1	Protocol de Kushilevitz i Ostrovsky	323
10.8.2	Protocol de Chor et al.	326
<b>10.9</b>	<b>Protocol multipart segur</b>	<b>328</b>
10.9.1	El problema del milionari	329
10.9.2	El problema del milionari socialista	330
<b>10.10</b>	<b>Resum</b>	<b>332</b>
<b>10.11</b>	<b>Solucions dels exercicis</b>	<b>333</b>
<b>10.12</b>	<b>Bibliografia</b>	<b>337</b>