

## ΠΕΡΙΕΧΟΜΕΝΑ

<b>1. Εισαγωγή</b> .....	1
1.1. Ορισμοί και ορολογία .....	2
1.1.1. Συμμετρικά και ασύμμετρα κρυπτοσυστήματα .....	4
1.1.2. Κρυπτογραφικές υπηρεσίες και πρωτόκολλα .....	9
1.1.3. Αρχές μέτρησης κρυπτογραφικής δύναμης .....	10
<b>2. Θεωρία αριθμών – Αλγεβρικές δομές</b> .....	15
2.1. Βασικές έννοιες της θεωρίας αριθμών .....	15
2.2. Αλγόριθμος του Ευκλείδη .....	23
2.3. Modular αριθμητική – Ομάδες .....	27
2.4. Επίλυση modular γραμμικών εξισώσεων .....	35
2.5. Δακτύλιοι – Σώματα .....	37
2.5.1. Πεπερασμένα σώματα τάξεως $p$ .....	42
2.5.2. Πεπερασμένα σώματα της μορφής $GF(2^n)$ .....	47
2.6. Κινέζικο θεώρημα υπολοίπων .....	50
2.6.1. Συστήματα γραμμικών ισοδυναμιών .....	53
2.7. Δυνάμεις στο $\mathbf{Z}_n^*$ .....	57
2.7.1. Modular εκθετοποίηση .....	61
2.8. Ασκήσεις .....	65
<b>3. Οι κρυπταλγόριθμοι και οι ιδιότητές τους</b> .....	67
3.1. Θεωρία της πληροφορίας .....	67
3.1.1. Υποδομή: πιθανότητες και πληροφορία .....	67
3.1.2. Η θεωρία της πληροφορίας και το κρυπτοσύστημα .....	70
3.1.3. Τέλεια μυστικότητα .....	71

3.1.4. Περίσσεια της γλώσσας και unicity distance .....	73
3.2. Ορολογία – παραστάσεις .....	74
3.2.1. Κρυπταλγόριθμοι ροής και κρυπταλγόριθμοι τμήματος .....	76
3.3. Κατηγορίες κρυπτογραφικών πράξεων .....	80
3.3.1. Αναδιάταξη .....	80
3.3.2. Μονοαλφαβητική αντικατάσταση .....	81
3.3.3. Πολυαλφαβητική αντικατάσταση .....	86
3.3.4. Ανίχνευση της γλώσσας .....	103
3.3.5. Κρυπτογράφηση γινομένου .....	106
3.4. Ασκήσεις .....	109
<b>4. Κρυπτογραφικές συναρτήσεις .....</b>	<b>111</b>
4.1. Εισαγωγή .....	111
4.2. Ψευδοτυχαίες ακολουθίες .....	111
4.2.1. Στατιστικοί έλεγχοι τυχαιότητας .....	112
4.2.2. Γεννήτριες ψευδοτυχαίων ακολουθιών .....	115
4.3. Μονόδρομες hash συναρτήσεις .....	125
4.3.1. Μέγεθος της σύνοψης .....	127
4.3.2. Αυθεντικοποίηση και ακεραιότητα ενός μηνύματος .....	129
4.4. Δίκτυα Αντικατάστασης – Μετάθεσης (ΔΑΜ) .....	141
4.4.1. Κουτιά αντικατάστασης .....	142
4.4.2. Δίκτυα Αντικατάστασης – Μετάθεσης με κλειδί .....	144
4.5. Δίκτυα Feistel .....	146
4.5.1. Ασφάλεια δικτύων Feistel .....	148
4.6. Ασκήσεις .....	155
<b>5. Συμμετρική κρυπτογραφία .....</b>	<b>157</b>
5.1. Εισαγωγή .....	157
5.2. Κρυπταλγόριθμοι τμήματος .....	157
5.2.1. Τρόποι λειτουργίας .....	158
5.2.2. Αλγόριθμοι προγράμματος κλειδιών .....	171
5.2.3. Γραμμική και διαφορική κρυπτανάλυση .....	173
5.2.4. Ο κρυπταλγόριθμος DES .....	183
5.2.5. Ο κρυπταλγόριθμος AES .....	196
5.3. Κρυπταλγόριθμοι ροής .....	201
5.3.1. Κλειδοροές βασισμένες σε καταχωρητές ολίσθησης με γραμμική ανάδραση .....	201

5.3.2.	Κρυπταλγόριθμοι ροής βασισμένοι στη θεωρία πολυπλοκότητας .....	204
5.3.3.	Ο κρυπταλγόριθμος RC4 .....	207
5.4.	Ασκήσεις .....	208
<b>6.</b>	<b>Ασύμμετρη κρυπτογραφία .....</b>	<b>211</b>
6.1.	Εισαγωγή .....	211
6.2.	Μονόδρομες συναρτήσεις με μυστική πόρτα .....	211
6.3.	Ο αντίπαλος .....	212
6.3.1.	Μοντέλα επίθεσης .....	213
6.4.	Κρυπτοσυστήματα knapsack .....	214
6.4.1.	Το κρυπτοσύστημα Merkle και Hellman .....	217
6.5.	Το κρυπτοσύστημα RSA .....	220
6.5.1.	Ανάλυση του RSA .....	222
6.5.2.	Ασφάλεια του RSA .....	226
6.6.	Το κρυπτοσύστημα ElGamal .....	228
6.6.1.	Ασφάλεια του ElGamal .....	229
6.7.	Κρυπτοσυστήματα ελλειπτικών καμπυλών .....	230
6.7.1.	Ελλειπτικές καμπύλες στο σώμα των πραγματικών αριθμών .....	230
6.7.2.	Οι ελλειπτικές καμπύλες ορισμένες modulo $p$ .....	236
6.7.3.	Οι ελλειπτικές καμπύλες ορισμένες σε $GF(2^n)$ .....	239
6.7.4.	Το πρόβλημα του διακριτού λογάριθμου στις ελλειπτικές καμπύλες .....	239
6.7.5.	Ασφάλεια των ελλειπτικών καμπυλών .....	241
6.7.6.	Κρυπτογραφία σε ελλειπτικές καμπύλες: ElGamal .....	242
6.8.	Ασκήσεις .....	243
<b>7.</b>	<b>Διαχείριση κλειδιών .....</b>	<b>245</b>
7.1.	Εισαγωγή .....	245
7.2.	Τύποι κλειδιών .....	246
7.3.	Ο αντίπαλος .....	247
7.4.	Εδραίωση κλειδιών .....	248
7.4.1.	Εδραίωση κλειδιών σε συμμετρικά κρυπτοσυστήματα .....	248
7.4.2.	Περαιτέρω εδραίωση κλειδιών χωρίς τη συμμετοχή του Κέντρου .....	256
7.4.3.	Το πρωτόκολλο αυθεντικοποίησης Κέρβερος .....	258

7.4.4.	Εδραίωση κλειδιών χωρίς την ύπαρξη Κέντρων .....	262
7.4.5.	Εδραίωση κλειδιών σε ασύμμετρα κρυπτοσυστήματα .....	263
7.5.	Διαμοιρασμός μυστικών και τεμαχισμός κλειδιών .....	268
7.5.1.	Σχέδια $(m,n)$ -κατωφλίου πολυωνύμου παρεμβολής .....	269
7.5.2.	Ασφάλεια σχεδίου $(m,n)$ -κατωφλίου πολυωνύμου παρεμβολής .....	270
7.6.	Υποδομές δημόσιου κλειδιού .....	271
7.6.1.	Συστατικά ενός PKI .....	272
7.6.2.	Μοντέλα εμπιστοσύνης .....	273
7.6.3.	Το πιστοποιητικό .....	277
7.6.4.	Διαδικασίες δημιουργίας, ελέγχου και ανάκλησης .....	279
7.7.	Ασκήσεις .....	283
<b>8.</b>	<b>Ψηφιακές υπογραφές</b> .....	<b>285</b>
8.1.	Εισαγωγή .....	285
8.2.	Απαιτήσεις – ορισμοί .....	285
8.3.	Ψηφιακές υπογραφές ασύμμετρης κρυπτογραφίας .....	289
8.3.1.	Σύστημα ψηφιακής υπογραφής με αυτοανάκτηση .....	290
8.3.2.	Σύστημα ψηφιακής υπογραφής με παράρτημα .....	292
8.3.3.	Ψηφιακές υπογραφές με το κρυπτοσύστημα RSA .....	293
8.3.4.	Το σύστημα ψηφιακών υπογραφών Fiege-Fiat-Shamir .....	296
8.3.5.	Το σύστημα ψηφιακών υπογραφών ElGamal .....	298
8.3.6.	Το Πρότυπο Ψηφιακής Υπογραφής (DSS) .....	300
8.3.7.	Συστήματα τυφλών ψηφιακών υπογραφών .....	302
8.4.	Ψηφιακές υπογραφές συμμετρικής κρυπτογραφίας .....	305
8.4.1.	Σύστημα ψηφιακής υπογραφής χωρίς τη συμμετοχή διαιτητή .....	305
8.4.2.	Σύστημα ψηφιακής υπογραφής με διαιτητή .....	307
<b>9.</b>	<b>Κρυπτογραφικά πρωτόκολλα</b> .....	<b>311</b>
9.1.	Εισαγωγή .....	311
9.2.	Ο αντίπαλος .....	312
9.2.1.	Ανάλυση των κρυπτογραφικών πρωτοκόλλων .....	313
9.3.	Κατηγορίες πρωτοκόλλων .....	314
9.4.	Παραδείγματα κρυπτογραφικών πρωτοκόλλων .....	315
9.4.1.	«Νοερό πόκερ» .....	315
9.4.2.	Bit πρωτόκολλα δέσμευσης .....	317

9.4.3. Ρίψη κέρματος .....	319
9.4.4. Μεταφορά εν αγνοία .....	320
9.4.5. Υπογραφή συμβολαίου .....	322
9.5. Πρωτόκολλα αυθεντικοποίησης ταυτότητας .....	324
9.5.1. Κατηγορίες αναγνώρισης .....	324
9.5.2. Εξουσιοδότηση .....	326
9.5.3. Αυθεντικοποίηση με κωδικούς πρόσβασης .....	326
9.5.4. Αυθεντικοποίηση με ψηφιακές υπογραφές .....	329
9.6. Πρωτόκολλα μηδενικής γνώσης .....	331
9.6.1. Δομή πρωτοκόλλου μηδενικής γνώσης .....	333
9.6.2. Πρωτόκολλο αυθεντικοποίησης των Fiat και Shamir .....	333
9.6.3. Πρωτόκολλο αυθεντικοποίησης των Guillou και Quisquar- ter .....	335
9.6.4. Πρωτόκολλο αυθεντικοποίησης του Schnorr .....	336
9.6.5. Πρωτόκολλα μηδενικής γνώσης βασισμένα στη θεωρία γράφων .....	338
9.7. Ασκήσεις .....	340
<b>ΠΑΡΑΡΤΗΜΑ</b>	
<b>A. Μαθηματικό υπόβαθρο</b> .....	341
A.1. Σύνολα .....	341
A.2. Συναρτήσεις .....	344
A.3. Διμελείς σχέσεις .....	349
A.4. Εσωτερικές πράξεις .....	352
A.5. Εσωτερική πράξη και κλάση ισοδυναμίας .....	354
A.6. Δομές – Ισομορφισμοί .....	356
A.7. Μεταθέσεις .....	359
A.8. Συνδυαστική – Πιθανότητες .....	361
<b>Βιβλιογραφία</b> .....	379
<b>Ευρετήριο</b> .....	389