ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ 7

ΚΕΦΑΛΑΙΟ 1.
ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ 11

1.1 ΕΙΔΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ 12
1.1.1 Ασύμμετρη Κρυπτογραφία 12
1.1.2 Συμμετρική Κρυπτογραφία 13
1.1.3 Μειονεκτήματα και Πλεονεκτήματα 14
1.2 ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΕΡΓΑΛΕΙΑ 15
1.2.1 Κώδικες Τμήματος 16
1.2.2 Τρόποι Λειτουργίας 17
1.2.3 Κώδικες Ροής 21
1.2.4 One-time Pads 21
1.2.5 Συναρτήσεις Κατακερματισμού 23
1.2.6 Message Authentication Code (MAC) 25
1.2.7 Μηχανισμοί Διαχείρισης και Ανταλλαγής Κλειδιών 26
1.3 ΑΠΛΕΣ ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ 26
1.3.1 Διαφύλαξη του Απορρήτου και Κρυπτογράφηση 26
1.3.2 Πιστοποίηση Ταυτότητας και Ψηφιακές Υπογραφές 27
1.4 ΜΗΧΑΝΙΣΜΟΙ ΚΑΙ ΑΛΓΟΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ 28
1.4.1 Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας 28
1.4.2 Αλγόριθμοι Συμμετρικής Κρυπτογραφίας 30
1.4.3 Συναρτήσεις Κατακερματισμού 33
1.4.4 Αλγόριθμοι για τη Διαχείριση και Ανταλλαγή Κλειδιών 34
1.4.5 Αρχές Έκδοσης Πιστοποιητικών 37
1.5 CRYPTOOL 39
ΕΡΓΑΣΤΗΡΙΑΚΕΣ ΑΣΚΗΣΕΙΣ 40
ΑΝΑΦΟΡΕΣ 42

ΚΕΦΑΛΑΙΟ 2.
ΔΙΑΧΕΙΡΙΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ - OPENSSL 43

2.1 Η ΒΙΒΛΙΟΘΗΚΗ ΚΑΙ ΤΑ ΕΡΓΑΛΕΙΑ OPENSSL 43
2.2 ΜΟΡΦΕΣ ΑΡΧΕΙΩΝ ΕΙΣΟΔΟΥ ΚΑΙ ΕΞΟΔΟΥ 47

2.3 ΠΡΟΤΥΠΑ ΕΛΕΓΧΟΥ ΑΝΑΚΛΗΘΕΝΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ....48
2.4 ΤΑ ΠΡΟΤΥΠΑ PKCS ΑΠΟ RSA LABS....48
ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΡΓΑΣΤΗΡΙΟΥ....49
ΕΡΓΑΣΤΗΡΙΑΚΕΣ ΑΣΚΗΣΕΙΣ....55
ΑΝΑΦΟΡΕΣ....58

ΚΕΦΑΛΑΙΟ 3.
ΒΟΗΘΗΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ – ΥΠΗΡΕΣΙΑ ΚΑΤΑΛΟΓΟΥ....59

3.1 LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)60
3.2 Η ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ LDAP....62
3.3 LDAP BROWSER....63
3.4 ΧΡΗΣΗ ΕΝΤΟΛΩΝ OPENLDAP....63
3.5 ΤΑ ΑΡΧΕΙΑ ΔΙΑΜΟΡΦΩΣΗΣ OPENLDAP....65
ΕΡΓΑΣΤΗΡΙΑΚΕΣ ΑΣΚΗΣΕΙΣ....66
ΑΝΑΦΟΡΕΣ....67

ΚΕΦΑΛΑΙΟ 4.
ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΚΛΕΙΔΙΩΝ – KEYTOOL....69

4.1 ΠΕΡΙΓΡΑΦΗ KEYTOOL....69
4.2 ΓΕΝΙΚΗ ΧΡΗΣΗ KEYTOOL....71
ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΡΓΑΣΤΗΡΙΟΥ....73
ΕΡΓΑΣΤΗΡΙΑΚΕΣ ΑΣΚΗΣΕΙΣ....74
ΑΝΑΦΟΡΕΣ....76

ΚΕΦΑΛΑΙΟ 5.
XML– WEB SERVICES....77

5.1 ΕΙΣΑΓΩΓΗ....77
5.2 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ....79
5.3 XML ΚΡΥΠΤΟΓΡΑΦΗΣΗ....81
5.4 ΥΠΗΡΕΣΙΕΣ ΙΣΤΟΥ....83
5.5 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΥΠΗΡΕΣΙΩΝ ΙΣΤΟΥ....86
5.6 ΕΠΕΚΤΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΥΠΗΡΕΣΙΩΝ ΙΣΤΟΥ (WS-SECURITY)....88
5.7 ΕΡΓΑΛΕΙΑ....91
ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΡΓΑΣΤΗΡΙΟΥ....92

ΕΡΓΑΣΤΗΡΙΑΚΕΣ ΑΣΚΗΣΕΙΣ 93
ΑΝΑΦΟΡΕΣ 93

ΚΕΦΑΛΑΙΟ 6.
ΔΙΚΤΥΑΚΗ ΑΣΦΑΛΕΙΑ 95

6.1 ΕΙΣΑΓΩΓΗ 95
6.2 ΕΝΟΤΗΤΑ 1: TCPDUMP 95
6.2.1 Εισαγωγή 95
6.2.2 Παραδείγματα Εργαστηρίου 99
6.2.3 Εργαστηριακές Ασκήσεις 102
6.3 ΕΝΟΤΗΤΑ 2: NETFILTER / IPTABLES 106
6.3.1 Εισαγωγή 106
6.3.2 Παραδείγματα Εργαστηρίου 110
6.3.3 Εργαστηριακές Ασκήσεις 113
6.4 ΕΝΟΤΗΤΑ 3 - SNORT 117
6.4.1 Εισαγωγή 117
6.4.2 Περιγραφή του Snort 118
6.4.3 Εργαστηριακές Ασκήσεις 121
ΑΝΑΦΟΡΕΣ 122