Contents

THE MINISTRY OF EDUCATION AND RESEARCH FOREWORD 15

THE ACADEMY OF ECONOMIC STUDIES FOREWORD 17

THE ECONOMIC INFORMATICS DEPARTMENT FOREWORD ... 19

THE INFORMATICS SECURITY MASTER FOREWORD.............. 21

***MODULE 1* – CRYPTOGRAPHY BASIS.. 25**

1. Introduction to Cryptography 25

1.1 Basic Concepts 25
1.2 Algorithms Issues and Classifications 26
1.2.1 Random numbers generators used in cryptography 26
1.2.2 Algorithms before 70's..28
1.2.3 Hash functions used in cryptography 29
1.2.4 Symmetric cryptographic systems 30
1.2.5 Asymmetric cryptographic systems 32
1.3 Conclusions..34
References: 34

2. Symmetric crypto-algorithms' ancestor issues..35

2.1 Transposition ciphers 35
2.2 Substitution ciphers...37
2.2.1 Mono alphabetic substitutions...38
2.2.2 Homophonic and poly alphabetic substitutions 41
2.2.3 Polygramic substitutions 43
2.3 Items of computational complex ciphers 45
2.4 Conclusions..47
References: 47

3. Issues of MD5 – hash algorithm and Data Encryption Standard – symmetric key algorithm 49

3.1 MD5 description 49
3.2 DES Data Encryption Standard description..51

3.3 Conclusions 58

4. Practical topics on Rijndael - Advanced Encryption Standard - AES, symmetric key algorithm 59
4.1 Mathematical Preliminaries in Rijndael 59
4.2 Designing the architecture of Rijndael algorithm 64
4.3 Rijndael Cipher 66
4.4 Rijndael Reverse Cipher 72
4.5 Conclusions 74
References: 74

5. Simple Approach on MH, RSA, El Gammal and DSS, asymmetric key algorithms 75
5.1 The MH – Merkle and Hellman – with addition trapdoor 75
5.2 RSA – Rivest, Shamir, Adleman 77
5.3 El Gammal 79
5.4 DSS – Digital Signature Standard 80
5.5 Conclusions 82
References: 82

6. Encryption Modes and Multiple Ciphers used in Cryptography 83
6.1 Encryption modes 83
6.2 Block ciphers 84
6.2.1 ECB encryption - Electronic Codebook 84
6.2.2 CBC encryption - Cipher Block Chaining 85
6.2.3 PCBC encryption – Propagation Cipher Block Chaining 86
6.3 Stream ciphers 87
6.4 Multiple ciphering systems 89
6.5 Conclusions 90
References: 91

7. Secret Sharing Schemes 93
7.1 Introduction 93
7.2 Secret Splitting 94
7.2.1 Partial Information Disclosure 95
7.2.2 Modifying Disclosure Conditions 97
7.2.3 (k, n) - Secret Sharing 98
7.3 Construction of Secret Sharing Systems 99
7.3.1 Threshold Secret Sharing Systems 99
7.3.2 Unanimous Consent Schemes 106
7.3.3 Secret Sharing for Graph-based Access Structures 107
7.3.4 Weighted Threshold Secret Sharing Schemes 108
7.3.6 Compartmented Secret Sharing Schemes 116
7.3.7 General Secret Sharing Schemes 120
7.4 On-line Secret Sharing 129
7.4.1 Proactive Secret Sharing 130

7.4.2 Proactive (k, n) Secret Sharing 132
7.5 Appendix 133
7.5.1 The Chinese Remainder Theorem 133
References: 135

MODULE 2 – ELECTRONIC SIGNATURES 155

1. An Overview of Electronic Signatures Technology 155
1.1 Information security and education needs 155
1.2 Electronic signatures technology 156
Encryption 157
Public Key Cryptography 157
Digital Signatures 157
Certificates 158
Policies 159
Key Management—PKI 159
1.3 Electronic signatures applications 161
1.4 European Electronic Signature Initiative 164
1.5 Electronic signature and the legal acceptance 168
1.6 Conclusions 170
References: 170

2. Practical Approaches on Heterogenous Electronic Signatures Implementations 171
2.1 RSA authentication, confidentiality and digital signature 171
2.2 Dual and Blind Signatures 177
2.3 XML Signature 181
2.4 Conclusions 183
References: 183

MODULE 3 – SECURITY STANDARDS AND PROTOCOLS....... 187

1. Overview of security protocols and standards 187
1.1 Cryptography standards 187
1.2 Authentication protocols 194
1.3 Network layer security protocols 195
1.4 Transport layer security protocols 197
1.5 Application layer security protocols 198
1.6 Conclusions 203
References: 203

2. Details Issues on PKCSs 205
2.1 PKCS Types 205
2.2 PKCS #1 Description 207
2.3 Conclusions 214

References: 214

MODULE 4 – SECURE APPLICATIONS PROGRAMMING 219

1. Info Foundation – ASN.1 vs XML and Encodings 219
1.1 ASN.1 – Abstract Syntax Notation 219
1.2 XML – eXtended Markup Language Technology 227
1.3 Encoding Data 233
1.4 Conclusions 237
References: 238

2. Practical Approach on X509 Certificates and PKIs 239
2.1 Certificates and certification 239
2.2 The format of X509 v3 Digital Certificate 240
2.3 Protocols for the Certificates Management 252
2.3 Conclusions 253
References: 254

MODULE 5 – SECURITY IN OPERATING SYSTEMS 257

1. Issues of security in operating systems 257
1.1 Introduction 257
1.2 Computer System Assets 259
1.3 Design principles 260
1.4 Protection mechanism 261
1.4.1 Memory Protection 262
1.4.2 Protecting objects 262
1.4.3 Protection based on operating system mode 269
1.5 File sharing 271
1.6 Trusted systems 272
1.7 Windows Operating System security 274
References: 278

MODULE 6 – INTERNET AND GRID COMPUTING SECURITY 281

1. Practical Approach on TCP/IP Application Layer Protocols 281
1.1 HTTP Protocol and Trafic Analysis 281
1.2 SMTP Protocol and Trafic Analysis 285
1.3 FTP Protocol and Trafic Analysis 288
1.4 Web Services Protocols and Trafic Analysis 292
References: 303

MODULE 7 – OBJECT ORIENTED PROGRAMMING IN DISTRIBUTED APPLICATION DEVELOPMENT 307

1. Practical Approach on SSL from TCP/IP Protocols..**307**
1.1 TCP/IP Security Overview..307
1.2 SSL/TSL - HTTPS 309
1.3 Conclusions...322
References: 323

MODULE 8 – SECURE DISTRIBUTED SYSTEMS DEVELOPMENT 327

1. Overview on concepts, design and use of security in distributed systems **327**
1.1 The traditional view of parallel and distributed systems 327
1.2 Design issues of parallel and distributed systems 329
1.3 RPC and RMI - Remote Procedure Call and Remote Object Invocation 333
1.4 Secure RPC 340
1.5 Middleware security and layering of security mechanism 341
1.6 Session-level security, group security, secure replicated services and design issues..345
1.7 Java security...347
1.8 Conclusions...347
References: 348

MODULE 9 – E-COMMERCE AND E-PAYMENT SECURITY 353

1. E-Commerce and E-payments Secure Technologies....................................**353**
1.1 E-Commerce security needs...353
1.2 E-Commerce security principles..354
1.3 Electronic payments 357
1.4 Conclusions...364
References: 364

2. Tutorial on Java Smart-Card Electronic Wallet Application **365**
2.1 Introduction..365
2.2 Complete applications for Java smart cards 366
2.3 Elements involved in the development and life cycle of a Java card applet...371
2.4 Practical sample of developing a Java applet card 376
2.5 Conclusions...383
References: 383

3. Secure Patterns and Smart-card Technologies used in e-Commerce, e-Payment and e-Government..**393**

3.1 Introduction 393
3.2 Smart-card technologies 394
3.3 Java technologies for smart-cards 396
3.4 E-commerce and security features 398
3.5 Analysis of SET – Secure Electronic Transaction 399
3.6 Conclusions 408
References: 408

4. On-line Payment System e-Cash 411
4.1 Introduction 411
4.2 Electronic money and payment electronic system features 412
4.3 Electronic payment mechanism 414
4.4 E-cash payment system 416
4.5 Conclusions 420
References: 421

***MODULE 10* – VIRUSES AND ANTI-VIRUSES TECHNOLOGIES 425**

1. Developing viruses and anti-viruses 425
1.1 Course Overview 425
1.2 Viruses Features 426
1.3 COM files features 427
1.4 COM files viruse – MINI44 430
1.5 Anti-viruses features 433
References: 434

***MODULE 11* – SOURCE CODE PROGRAMMING SECURITY.... 437**

1. Writing Secure Code 437
1.1 Course Overview 437
1.2 Buffer overflows 438
1.3 SQL Injection 441
1.4 Protecting program code from reverse engineering 444
1.5 Key Components of the .NET Security System 446
1.6 Denial of Service at Application Level 447
1.7 Conclusions 447
References: 448

***MODULE 12* – MOBILE APPLICATION SECURITY 451**

1. WiFi Security 451
1.1 WiFi Intro 451
1.2 WiFi Security 453

1.3 WEP Encryption / Decryption 454
1.4 WEP Authentication 459
References: 462

2. GSM Security and Non-repudiation WAP Solution 463
2.1 GSM Network Overview 463
2.2 GSM Voice and Data Security 465
2.3 SAWNR Solution 468
References: 473

***MODULE 13* – INFORMATICS PROJECT MANAGEMENT 477**

1. E-commerce Project Management 477
1.1 Introduction 477
1.2 The role of eCommerce projects management in company life 478
1.3 The dimensions of management in eCommerce projects 481
1.4 eCommerce security features 484
1.5 Conclusions 485
References: 486

***MODULE 14* – MULTIAGENT SECURITY SYSTEMS 489**

1. Mobile Agent Security Systems in Wireless Applications 489
1.1 Introduction and background of wireless and mobile applications 489
1.2 Mobile agents clasificassion and their integration in mobile applications 491
1.3 Privacy and security in mobile applications 496
1.4 Conclusions 498
References: 499

***MODULE 15* – AUDIT AND EVALUATION OF THE SECURITY SYSTEMS 503**

1. Audit and Evaluation Issues of the Information System Security 503
1.1 Information Systems 503
1.2 Characteristics of the Audit for Information Systems 510
1.3 Audit Standards for Information System Security 514
1.5 Conclusions 520
References: 520

***MODULE 16* – RISK ANALYSIS IN SECURED SYSTEMS 525**

1. Features of Risk Analysis in Secured Systems 525
1.1 Introduction 525

1.2 Items involved in risk analysis 526
1.3 Conclusions 535
References: 536

***MODULE 17* – INFORMATICS ETHIC CODES 539**

1. Overview of Informatics Ethic Codes 539
1.1 Professions in informatics 539
1.2 Professions in informatics products utilization 542
1.3 Informatics Risks 544
1.4 Ethic codes 547
1.5 The developer ethic code 550
1.6 The ethic codes system 557
1.7 Conclusions 560
References: 560

***MODULE 18* – DATABASES, DATAWAREHOUSES AND DATAMINING SECURITY 565**

1. Overview on Databases Security 565
1.1 Introduction 565
1.2 Database integrity 568
1.3 Security techniques and security of multilevel database 569
1.4 Architectures for insuring database security 574
References: 575

***MODULE 19* – LEGISLATION OF INFORMATICS SECURITY SYSTEMS 579**

1. Informatics Security Systems Legislation 579
1.1 Software products features 579
1.2 The copyright of software products 582
1.3 The property of software products 584
1.4 The right of use of software products 585
1.5 Automatization process 587
1.6 Software piracy 588
1.7 Conclusions 591
References: 591

***MODULE 20* – IT&C SECURITY COMPANIES SECTION 595**

1. SATS – Secure Automatic Ticketing System 595
1.1 Introduction 595

1.2 SATS Concepts 596
1.3 SATS Concepts 599
1.4 Conclusions 601
References: 602

2. DECWEB - Internet fiscal statement submission 603
2.1 Project overview and objectives 603
2.2 Project details 605
2.3 Impact of project 609
2.4 Outlook 610
References: 612

3. Security Issues Applied in SPGBP – Simmulation of Proteins Generation Bioinformatic Project 615
3.1 Distributed Architecture of SPGBP 615
3.2 SPGBP Communication Protocols and Parallel Processing 618
3.3 Bioinformatics Concepts in SPGBP 627
3.4 Security Issues and Research Directions 643
References: 646

BIBLIOGRAPHY 647

ANNEX 1 – INFORMATICS SECURITY MASTER CURRICULA ... 653

ANNEX 2 – SURNAME INDEX OF AUTHORS INVOLVED IN INFORMATICS/IT&C SECURITY MASTER 655

ANNEX 3 – THE CONFERENCES PROMOTED BY ISM 659

ANNEX 4 – INFORMATICS SECURITY MASTER CONTACT 663