# A. Basic Information

**Course Title**: Computer Security **Code**: CSE443
**Lecture**: 4 **Tutorial**: 2 **Practical**: - **Total:** 6
**Program on which the course is given:** B.Sc. Electrical Engineering (Computers)
**Major or minor element of program:** Major
**Department offering the program:** Electrical Engineering Department
**Department offering the course:** Electrical Engineering Department
**Academic year / level:** **Fourth** Year / **Second** Semester
**Date of specifications approval :**

# B. Professional Information

## 1. Overall aims of course

By the end of the course the students will be able to:

Understand the principles of computer information security in general and the techniques of constructing secure systems in particular. It familiarizes students with the aspects of information security: security attacks, security mechanisms, and security services. Since cryptographic techniques underlie many of the security mechanisms in use, this course covers the development, use and management of such techniques. It also introduces authentication techniques, access control mechanisms, and how security assurance is achieved on computer networks. The course will cover a wide coverage for the tools needed to protect computer systems from both inside attacks and network based attacks. Theory and applications of various techniques will be explored. Analyze different cryptographic protocols in computer security, ways of hardening a system against computer attacks, implement security services on network systems such as User authentication, network security, intrusion detection systems, etc.

.٢

**2- Intended learning outcomes of course (ILOs)**

By completion of the course, the student should be able to:

**a. Knowledge and Understanding**

a.1)Concepts and theories of information security.
a.5) Methodologies of solving engineering problems, data collection interpretation.
a.7) Business and management principles relevant to engineering.
a.8) Current engineering technologies as related to disciplines.
a.13) Essential facts, concepts, principles and theories relevant to computer security.
a.17) Modern trends in information security and its fundamental role in business enterprises.

**b. Intellectual Skills**

b.13) Demonstrate a high level of competence in identifying, defining and solving computer engineering problems;
b.14) Select and apply appropriate mathematical tools, computing methods, design techniques and tools in computer engineering disciplines, for modeling and analyzing the security of computer systems.
b.16) Identifying symptoms in problematic situations.

**c. Professional and Practical Skills**

c.16) Write computer programs
c.17) Integrate technical professionalism and societal and ethical responsibility

**d. General and Transferable Skills**

d.1) Collaborate effectively within multidisciplinary team.
d.3) Communicate effectively

### 3. Contents

| No | Topic | No. of hours | ILOs | Teaching / learning methods and strategies | Assessment method |
|---|---|---|---|---|---|
| 1 | Overview of Information Security | 3 | a.1, a.5, a.13,a.17 | Lecture and Lab | Quiz, assignment, mid-term and final exam |
| 2 | Attackers and their attacks | 3 | a.1, a.13,b.14 | Lecture and Lab | Quiz, assignment, mid-term and final exam |
| 3 | Security Basics | 3 | a.1, a.13,b.14 | Lecture and Lab | Quiz, assignment, mid-term and final exam |
| 4 | Mathematics of Cryptography [1] | 3 | a.1, a.5, a.13 | Lecture and Lab | Quiz, assignment, mid-term and final exam |
| 5 | Traditional Symmetric-Key Ciphers | 3 | a.1, a.5, a.13 | Lecture and Lab | Quiz, assignment, mid-term and final exam |
| 6 | Modern Symmetric-Key Ciphers | 3 | a.1, a.5, a.13, a.17 | Lecture and Lab | Quiz, assignment, mid-term and final exam |
| 7 | Encryption Using Symmetric-Key Cryptography DES | 3 | a.1, a.5, a.13, a.17, b.14 | Lecture and Lab | Quiz, assignment, mid-term and final exam |
| 8 | Mathematics of Cryptography [1] | 3 | a.1, a.5, a.13 | Lecture and Lab | Quiz, assignment, mid-term and final exam |

| | | | | | |
|---|---|---|---|---|---|
| 9 | Asymmetric Key Cryptography | 3 | a.5, a.13, a.17, b.14 | Lecture and Lab | Quiz, assignment, mid-term and final exam |
| 10 | Message Integrity and Authentication | 3 | a.5, a.13, a.17, b.13, b.14 | Lecture and Lab | Quiz, assignment, and final exam |
| 11 | Hash Functions and Digital Signature | 3 | a.5, a.13, a.17, b.13, b.14 | Lecture and Lab | Quiz, assignment, and final exam |
| 12 | Entity Authentication | 3 | a.5, a.13, a.17, b.13, b.14 | Lecture and Lab | Quiz, assignment, and final exam |
| 13 | Key Management | 3 | a.7, a.8, a.17 | Lecture and Lab | Quiz, assignment, and final exam |
| 14 | Revision | 3 | a.8, a.13, a.17 | Lecture and Lab | final exam sructure |
| | Final exam | | | | |

**4. Teaching and Learning Methods**

- Lectures
- laboratory
- Project Assignment

**5. Student Assessment Methods**

- Project Assignment to assess knowledge and intellectual skills.
- Laboratory assignments to assess knowledge, intellectual and professional skills.
- Mid-term exam to assess knowledge, intellectual, professional and general skills.
- Quizes to assess knowledge, intellectual, professional and general skills.
- Oral project presentation to assess knowledge and intellectual skills.
- Final exam to assess knowledge, intellectual, professional and general skills.

### 6. Assessment schedule

Assessment 1 on weeks 1,3,5,7,9
Assessment 2 Quizzes on weeks 2, 4, 6,10,12
Assessment 3 Mid-term exam on week 8
Assessment 4 Project on week 14
Assessment 5 Final exam on week 15

### 7. Weighting of Assessments

| | |
|---|---|
| Mid- Term Examination | 20% |
| Final- Term Examination | 60% |
| Project | 10% |
| Quizes (2) | 10% |
| Semester Work | 40% |
| Total | 100% |

### 8. List of References

8.1 **Course Notes**

NA

8.2 **Essential Books (Text Books)**

- Security+ Guide To NETWORK SECURITY Fundamentals, Second Edition, Mark Ciampa , Thomson Course Technology
- Introduction to CRYPTOGRAPHY and NETWORK SECURITY, Behrouz A.Forouzan , McGraw-Hill International Edition**.**

8.3 **Recommended books**

- Computer Security: Principles and Practice, William Stallings, Lawrie Brown, Prentice Hall, 2007, ISBN-10: 0136004245
- Principles of Computer Security , W.A.Conklin , D.Williams, G.White, R.Davis , C.Cothren, McGraw-Hill
- Anti-Hacker Tool Kit, Third Edition, Mike Shema, McGraw-Hill Osborne Media, third edition (February 9, 2006), ISBN: 0072262877.
- The Tao of Network Security Monitoring: Beyond Intrusion Detection by Richard Bejtlich, Addison-Wesley Professional, ISBN-10: 0321246772, ISBN-13: 978-0321246776

9.

9.1 Periodicals Web sites, etc

- Proceedings of the IEEE Symposium on Security and Privacy
- Proceedings of the ACM Conference on Computer and Communications Security
- Proceedings of the Annual Computer Security Applications Conference
- Usenix Proceedings
- Proceedings of the National Information Systems Security Conference
- IEEE Transactions on Software Engineering
- Computers and Security -- North Holland Publisher

- IEEE Computer Journal of Computer Security
- ACM Journal of Computer Security
- Journal of Cryptology

**10. Facilities Required for Teaching and learning**

- Lecture room equipped with overhead projector
- Presentation board, computer and data show

**11.** Laboratory

**Course coordinator:** Prof. Dr. **Mona F.M. Mursi**
**Course instructor:** Prof. Dr. **Mona F.M. Mursi**

**Head of department:** Prof. Dr. **Sayed A. Ward**