单词背诵表

这些词汇涵盖了电子商务信息安全领域的一些专业术语，有助于深入理解相关概念。

以下是词汇列表，包括它们在PDF中第一次出现的页码：

| 英文单词 | 中文释义 | 出现页码 |

|-----------------|----------------|--------|

| Cryptography | 加密技术 | 2 |

| Instructor | 讲师 | 2 |

| Teaching Assistant | 助教 | 2 |

| Plagiarism | 剽窃 | 6 |

| Symmetric | 对称的 | 9 |

| Asymmetric | 非对称的 | 9 |

| Non-repudiation | 不可抵赖性 | 9 |

| Mechanisms | 机制 | 9 |

| Countermeasures | 对策 | 9 |

| Vulnerabilities | 漏洞 | 9 |

| Adversaries | 敌手 | 9, 20 |

| Falsification | 伪造 | 9 |

| Masquerade | 伪装 | 9 |

| Repudiation | 抵赖 | 9 |

| Compliance | 遵从性 | 9 |

| Terminology | 术语 | 11 |

| Symmetric encryption | 对称加密 | 11 |

| Asymmetric Encryption | 非对称加密 | 11 |

| Adversary | 对手 | 20 |

| Circumvent | 规避克服 | 11 |

| Pry, snoop | 窥探 | 20 |

| Espionage | 间谍 | 20 |

| Breached | 违反 | 18 |

| Disclosure | 泄露 | 18 |

| CIA | 保密性、完整性、可用性 | 16 |

请注意，这些页码是根据PDF文档的顺序来标注的，实际的PDF阅读器或打印版可能会有所不同。

以下是更详细的知识提纲，适合背诵和复习：

1. \*\*Information Security for eCommerce\*\*

- 电子商务信息安全：保护在线交易和数据的安全性。

2. \*\*Teaching Materials\*\*

- 每周讲座幻灯片：提前几天在Canvas上发布，课后会附上额外评论。

- 教科书：William Stallings的《Cryptography and Network Security: Principles and Practices》（第3至8版）。

- 额外阅读和参考资料：核心工作在幻灯片中。

3. \*\*Weekly Teaching Pattern\*\*

- 讲座（2小时）：14:00-15:50，传统讲座，讨论设定阅读/案例研究。

- 辅导课（1小时）：16:00-16:50（AC5 416）或17:00-17:50（AC5 417），理论课程，纸质问题/练习，每周问题表。

- Canvas上的讨论：16:00-16:30/17:00-17:30开放讨论，16:30/17:30开始讨论辅导课解答。

4. \*\*Assessment\*\*

- 课程作业（40%）：2次家庭作业（各10%），分别在第6周和第13周提交。

- 中期测验（20%）：第7周（10月22日）进行。

- 期末考试（60%）：必须在期末考试中至少获得30%的分数。

5. \*\*Plagiarism\*\*

- 剽窃：不允许抄袭任何来源，必须正确引用/参考。

6. \*\*GenAI\*\*

- 编程任务或解决任何数值/逻辑问题时，学生不允许使用GenAI。

- 写作作业和报告中允许使用GenAI，但必须通过适当的引用和参考来确认其使用。

7. \*\*Intended Learning Outcomes\*\*

- 完成课程后，学生应能够：

1. 确定电子商务系统对数据保护的组织要求。

2. 展示对影响电子商务系统安全性的因素的知识。

3. 对电子商务系统的安全性进行批评和评估。

4. 描述管理电子交易、数据隐私保护和网络访问的相关法规。

5. 创建设计并分析保护电子商务系统和交易的安全机制。

8. \*\*Tentative Course Overview\*\*

- 第1周：行政和基本安全术语。

- 第2周：对称加密。

- 第4周：数论/非对称加密。

- 第5周：完整性。

- 第6周：认证（问题集1）。

- 第7周：中期测验。

- 第8-9周：密钥管理。

- 第10-12周：计算机安全和网络安全。

- 第13周：复习（问题集2）。

**9. \*\*Basic Security Goals (CIA)\*\***

**- 保密性（Confidentiality）：防止未经授权的信息披露。**

**- 完整性（Integrity）：防止未经授权的信息修改。**

**- 可用性（Availability）：防止未经授权的信息或资源扣留。**

**10. \*\*Threats\*\***

- 安全威胁：有deliberate和accidental，指可能破坏安全策略的手段，如数据泄露Exposure of data、篡改Tampering with data、拒绝服Denial of service。

**11. \*\*Adversaries\*\***

- 敌手：试图绕过安全措施的人，包括被动passive敌手（仅尝试获取未经授权的信息）和主动active敌手（采取更直接的行动，如未经授权的修改、删除、传输、伪造来源、未经授权的访问阻止）。

12. \*\*Security Services and Mechanisms\*\*

- 安全服务：应对威胁的措施，如提供保密性。

- 安全机制：提供服务的手段，如加密、数字签名。

13. \*\*Authentication\*\*

- 实体entity认证：在特定时间点验证声称的身份，通常用于连接开始时，解决伪装和重放威胁。

- 来源origin认证：验证数据的来源，不保护重放或延迟。

14. \*\*Access Control\*\*

- 访问控制：防止未经授权使用资源，包括通信资源、信息资源的读取、写入或删除、处理资源的执行。

**15. \*\*Non-repudiation\*\***

- 不可抵赖性：防止数据发送者否认发送数据（不可抵赖起源non-repudiation of origin），防止数据接收者否认接收数据（不可抵赖交付non-repudiation of delivery）。

16. \*\*Algorithms\*\*

- 算法：用于构建安全机制的方法，如加密算法（DES/3DES/AES、RSA/ECC）、MAC算法（CBC模式、HMAC）、数字签名算法（RSA、DSA、ECC）、哈希算法（SHA-3）、随机数生成算法（真随机或伪随机）。

17. \*\*Standards\*\*

- 标准：为特定活动和结果提供规则和指导的文件，旨在实现给定上下文中最大程度的秩序。

- 国际标准：如ISO、IEC、ITU。

- 北美标准：如IEEE、NIST、ANSI。

- 互联网标准：由IETF制定。

- 公司标准：如PKCS、SECG、PCI DSS。

这个提纲涵盖了电子商务信息安全课程的关键概念和术语，适合用于学习和复习。

引用自kimi.ai