Final Exam Revision for Introduction to Security and Forensics- week 7-12

Note:
The bullet points with red color are all examinable contents in both resit and examination. Bullet Points with black color are basic concepts you should know as a computer science student. Past exam papers are also available on the moodle.

Week 7

- Basic concepts (Data, Information Security, etc.)
- What Should a Security Policy and System Provide?
- Aspects of security (Security attacks , Security threats, Security-mechanisms , Security services)
- Security needs
- Security controls
- Existing security systems/protocols

- Properties of security ciphers
- Basic concepts , Cryptography (type of security, symmetric ciphers or asymmetric cyphers)
- Traditional ciphers/modern ciphers (additive cipher, one-time pad.)
- Block ciphers

Week 8

- Public-key ciphers
- RSA algorithm, implementation, security
- The Diffie-Hellman

Week 9

- Message authentication and Message authentication code (integrity)
- Hash functions
- Digital Signature

Week 10

- Symmetric-key Distribution
- Key Distribution Center (Definition, types of KDC)
- Session Keys

- Needham Schroeder Protocol
- Otway-Rees Protocol
- What is Kerberos?
- Why Kerberos? How Does Kerberos Work?
- Formal Description of Kerberos
- Kerberos Drawbacks
- Kerberos Realm
- Kerberos v4.Vs v5
- Kerberos Pro. vs Cons.

Week 11

- Public key infrastructure (x.509 PKI, CA and the tasks, Digital certificate)

- What is Zero-Knowledge Proofs?
- Why Zero-Knowledge Proofs
- Interactive Proofs
- Zero Knowledge proofs
- Application: Fiat-Shamir Protocol

Week 12

- What Is Access Control?
- Access Control Model
- Access Control Lists vs. Capability (and covert channel, types of covert channel)
- Unix Access Control