Subject: **Security & Privacy**

Summary: This exam will evaluate the student's undergraduate and junior graduate understanding of the fundamental concepts, terminologies, and theories of computer security and privacy; principles underlying common security controls; various types of threats and attacks on networks and software systems, how they work, and controls for dealing with them; security risk assessment and management, and human factors of privacy and security. The specific subjects to be addressed are provided as keywords below.

Keywords

- **Fundamental Security and Privacy Concepts**:
  - Security Concepts: Confidentiality, Integrity, Availability, Assets, Threats, Attacks
  - Privacy Concepts: Anonymity, Pseudonymity, Unlinkability, Unobservability
  - Design Principles for Security and Privacy
  - Attack Surfaces and Attack Trees
  - Security Strategies, Policies, and Implementations: Prevention, Detection, Recovery
  - Malware: Viruses, Worms, Trojans, Bots, Spam, Phishing, Backdoors, Rootkits
  - Users' Mental Models, Behaviours, and Attitudes Towards Security and Privacy
- **Cryptography:**
  - Symmetric vs. Asymmetric, Hashing, Digital Signatures, Key Management
- **Authentication and Access Control:**
  - User Authentication: Digital Identity, Trust, Passwords, Tokens, Biometrics, Usability Issues
  - Access Control Principles: Subjects, Objects, Access Rights, Role-Based vs. Attribute-Based
  - Trusted Computing and Multilevel Security
  - Applications of, and Attacks Against, Advanced Security Protocols (e.g., zero-knowledge, e-voting)
- **Database Security:**
  - Database Access Control, Inference Attacks
- **Network Security:**
  - Intrusion Detection, Firewalls, and Intrusion Prevention Systems
  - Internet Security Protocols and Standards: SSL, TLS, HTTPS, IPSec
  - Internet Authentication Applications: Kerberos, Certificates, Public-Key Infrastructure
  - Wireless Network Security and Mobile Device Security
- **Software Security:**
  - Secure Programming, Buffer Overflows, Handling Inputs (e.g., SQL injection, Cross-site scripting), Handling Outputs
  - Factors Influencing Software Security in Practice (e.g., organizational factors and the usability of security tools)
- **Hardware Security:**
  - Active vs. Passive Attacks, Invasive vs. Non-invasive Attacks
- **System Security:**
  - Operating Systems Security, Cloud Security, IoT Security
- **Security Management:**
  - Risk Assessment and Threat Modeling, Security Controls Plans, and Procedures, Security Evaluation and Assurance