1. **Basic Concepts:**
   - Define and explain the concepts of confidentiality, integrity, and availability (CIA) in the context of cybersecurity. Provide examples of how each aspect can be compromised in different scenarios.

2. **Threat Analysis:**
   - Research and analyze a recent cyber attack (e.g., ransomware, phishing) and write a report detailing the attack vector, impact, and mitigation strategies employed by the affected organization.

3. **Risk Assessment:**
   - Conduct a risk assessment for a hypothetical organization's IT infrastructure. Identify potential threats and vulnerabilities, assess the likelihood and impact of each threat, and propose risk mitigation strategies.

4. **Network Security:**
   - Design a secure network architecture for a small business, considering factors such as firewalls, intrusion detection/prevention systems, VPNs, and secure remote access.

5. **Cryptography:**
   - Implement a simple encryption/decryption algorithm (e.g., Caesar cipher, XOR cipher) in a programming language of your choice. Demonstrate its effectiveness and discuss potential weaknesses.

6. **Security Policies and Procedures:**
   - Develop a set of security policies and procedures for an organization, covering areas such as acceptable use of resources, password management, incident response, and data backup