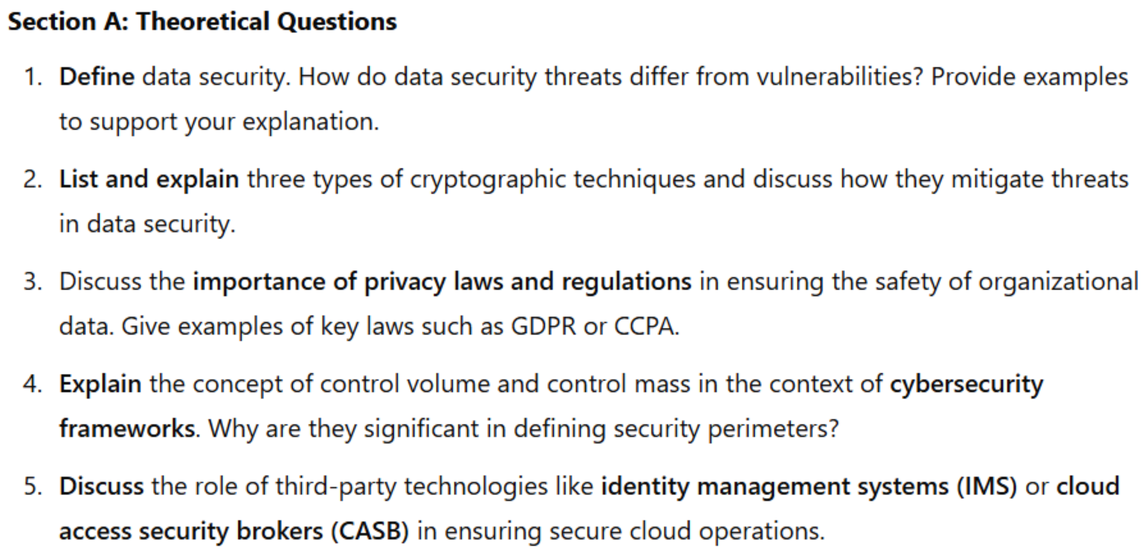
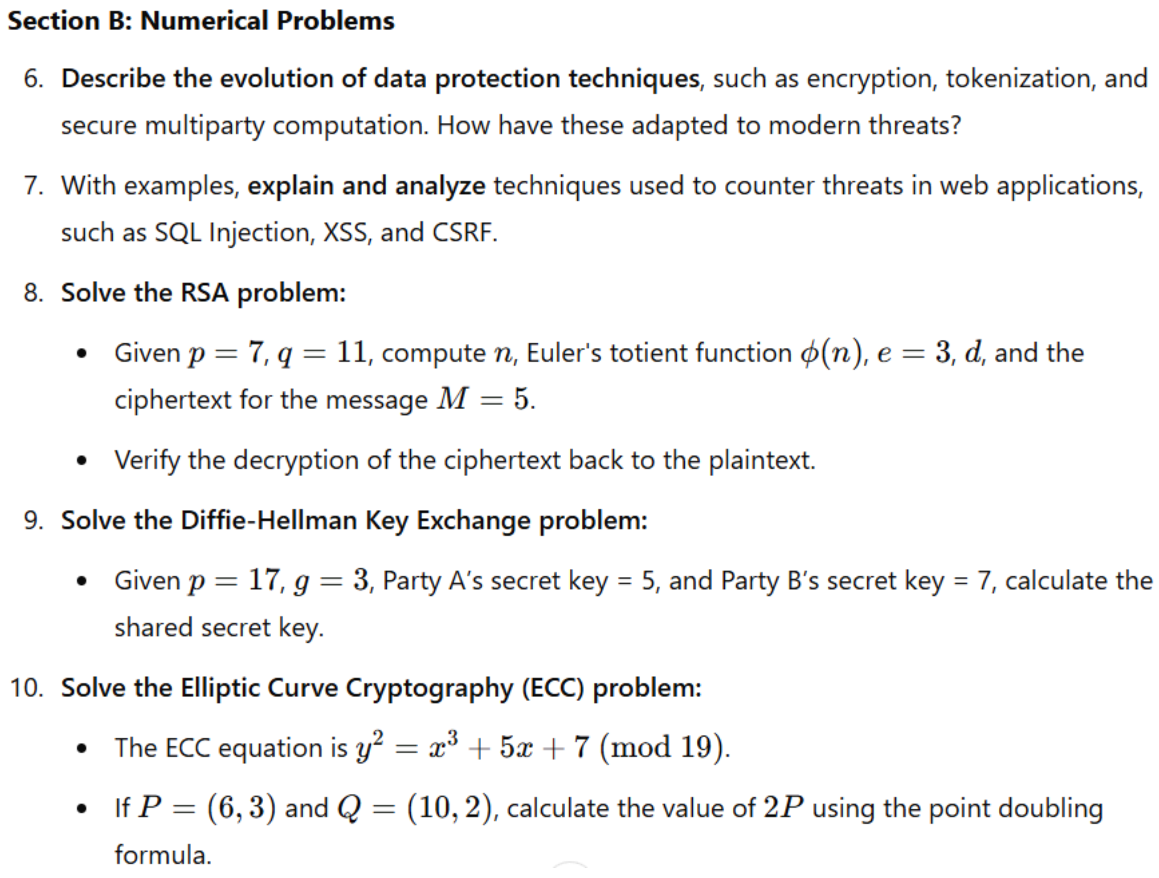
IT DATA SECURITY ASSIGNMENT



Section A: Theoretical Questions

1. **Define** data security. How do data security threats differ from vulnerabilities? Provide examples to support your explanation.
2. **List and explain** three types of cryptographic techniques and discuss how they mitigate threats in data security.
3. Discuss the **importance of privacy laws and regulations** in ensuring the safety of organizational data. Give examples of key laws such as GDPR or CCPA.
4. **Explain** the concept of control volume and control mass in the context of **cybersecurity frameworks**. Why are they significant in defining security perimeters?
5. **Discuss** the role of third-party technologies like **identity management systems (IMS)** or **cloud access security brokers (CASB)** in ensuring secure cloud operations.



Section B: Numerical Problems

6. **Describe the evolution of data protection techniques**, such as encryption, tokenization, and secure multiparty computation. How have these adapted to modern threats?
7. With examples, **explain and analyze** techniques used to counter threats in web applications, such as SQL Injection, XSS, and CSRF.
8. **Solve the RSA problem:**
   - Given $p = 7$, $q = 11$, compute n, Euler's totient function $\phi(n)$, $e = 3$, d, and the ciphertext for the message $M = 5$.
   - Verify the decryption of the ciphertext back to the plaintext.
9. **Solve the Diffie-Hellman Key Exchange problem:**
   - Given $p = 17$, $g = 3$, Party A's secret key = 5, and Party B's secret key = 7, calculate the shared secret key.
10. **Solve the Elliptic Curve Cryptography (ECC) problem:**
    - The ECC equation is $y^2 = x^3 + 5x + 7 \pmod{19}$.
    - If $P = (6, 3)$ and $Q = (10, 2)$, calculate the value of $2P$ using the point doubling formula.