Lab Assignment: Research-Based Writing on Advanced Cryptography

Objective

To explore advanced cryptography concepts in depth, evaluate their real-world applications, and critically assess the strengths and limitations of modern cryptographic tools.

Answer any THREE of the following research-based writing prompts. Your responses should demonstrate understanding of the topic, include real-world examples or current events, and cite at least one credible source per question (e.g., academic journals, cybersecurity blogs, vendor whitepapers, or government documentation).

Research Writing Prompts (Choose 3)

1. **Digital Certificates and Trust**
   Research how digital certificates are used to establish trust in e-commerce or government websites. Why is the certificate chain important? Include a real-world case where a certificate was misused or spoofed.
2. **The Role of PKI in Modern Infrastructure**
   Explore how Public Key Infrastructure (PKI) is implemented in enterprises today. What challenges do organizations face when managing PKI, and how are these challenges addressed?
3. **TLS vs. IPSec: Use Cases and Security Strengths**
   Compare and contrast TLS and IPSec in terms of their use cases and layers of the OSI model they operate on. Which protocol would you recommend for securing VoIP traffic and why?
4. **Key Management Strategies**
   Investigate the lifecycle of cryptographic keys. Why is key escrow controversial, and how does it relate to government access or law enforcement backdoors?
5. **Trust Models in Practice**
   Analyze the strengths and weaknesses of hierarchical, distributed, and bridge trust models. Which model best fits the needs of a global organization with multiple regional branches?
6. **Encryption Modes and Real-World Breaches**
   Discuss the role of block cipher modes (such as CBC or GCM) in ensuring secure encryption. Include a summary of a data breach that occurred due to improper implementation of a cipher mode