Tutorial Session 5

1. Automated Teller Machines (ATMs) play a vital role in modern banking, providing customers with convenient access to financial services. Suppose that a prominent bank operates an extensive network of ATMs across various locations, enabling customers to perform transactions such as cash withdrawals, balance inquiries, fund transfers, and more. Lately, the bank has experienced a surge in security incidents concerning their ATM network.
    i. How do card skimming devices compromise the security of ATM transactions, and what measures can banks take to detect and prevent skimming attacks?
    ii. Describe the potential consequences of cash trapping incidents for both customers and the bank, and outline strategies to mitigate this security issue.
    iii. What are the common types of malware attacks that target ATM systems, and how can banks enhance their software security to prevent such attacks?
    iv. How does two-factor authentication contribute to strengthening ATM transaction security? Provide examples of effective two-factor authentication methods for ATM users.
    v. Discuss the role of customer education in ATM security. What best practices can customers be encouraged to follow to minimize the risk of falling victim to security threats?
    vi. What challenges do banks face when it comes to implementing security measures across a widespread network of ATMs? How can these challenges be addressed effectively?
2. A large multinational corporation has implemented an IRIS biometric authentication system to secure access to sensitive areas within their offices. Employees use the system to enter restricted zones, access confidential data, and perform various tasks. However, the company has observed several problems and concerns related to the effectiveness, usability, and security of the IRIS biometric system.
    i. How do inconsistent false acceptance and false rejection rates affect the overall security and user experience of the IRIS biometric authentication system?

ii. Explain the potential impact of environmental factors, such as lighting and humidity, on the accuracy and reliability of the IRIS biometric system. What measures can be taken to mitigate these effects?

iii. What challenges might employees face during the enrolment process of the IRIS biometric system, and how can these challenges be addressed to ensure accurate and reliable iris data collection?

iv. Discuss the implications of extended authentication times in the context of the IRIS biometric system. How could slower authentication impact operational efficiency and user satisfaction?

3. Explain the suitability or unsuitability of the following passwords:
   i. YK 334
   ii. mfmitm
   iii. Natalie1
   iv. Washington
   v. Aristotle
   vi. tv9stove
   vii. 12345678
   viii. dribgib