Certainly! Below is the same content presented in a clear `Question:` / `Answer:` format for each type of exam question:

◇ 1-Mark Questions

Question 1: What is key management in cryptography?
Answer: It refers to the process of managing cryptographic keys, including their generation, exchange, storage, use, and destruction.

Question 2: Define Hierarchical Key Management.
Answer: It is a key management scheme where keys are arranged in a hierarchy, reducing the number of keys needed for secure communication.

Question 3: What does RBAC stand for?
Answer: Role-Based Access Control.

Question 4: Give one example of a physical access control.
Answer: Biometric door lock.

Question 5: What is the primary goal of access control?
Answer: To restrict unauthorized access to systems or resources.

◇ 5-Mark Questions

Question 1: Explain the concept of Hierarchical Key Management with an example.
Answer: Hierarchical Key Management organizes keys into a tree structure, where higher-level keys derive lower-level keys. For example, an organization might use a root key to generate department-level keys, which then generate user-level keys. This limits key distribution scope and enhances scalability.

Question 2: Differentiate between RBAC and ABAC.
Answer:

- RBAC (Role-Based Access Control) grants access based on a user's role, such as 'admin' or 'editor'.
- ABAC (Attribute-Based Access Control) considers attributes like time of access, location, and user status, offering more granular control.

Question 3: List and explain any three physical access control mechanisms.
Answer:

1. **Keycard entry systems** – Allow access with an electronic card.
2. **Biometric scanners** – Use fingerprints or facial recognition.
3. **Surveillance systems** – Monitor access points and deter intrusion.

Question 4: What are the key components of a User Authentication Protocol?
Answer: The key components are identification (e.g., username), authentication (e.g., password or token), and authorization (permissions granted post-login).

◇ 10-Mark Questions

Question 1: Describe various Key Management Schemes. Highlight the advantages of Hierarchical Key Management.
Answer:
Key management schemes include manual key distribution, centralized key management, and hierarchical schemes.
Hierarchical Key Management reduces complexity by structuring keys into a tree or layered model. For example, a network administrator manages a top-level key, which can be used to derive keys for departments and further down to individuals. This makes key updates and revocations more manageable and minimizes the impact of key compromise.

Question 2: Explain Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) in detail.
Answer:
RBAC assigns permissions based on a user's role, simplifying management in structured environments. For example, all "managers" have access to payroll data.
ABAC evaluates multiple attributes (e.g., user location, device, time of access) for dynamic and context-aware decisions. It supports policies like: “A user can access HR data only during work hours from the office network.” ABAC offers more flexibility but is complex to implement.

Question 3: Discuss User Authentication Protocols and their importance in securing systems.
Answer:
Authentication protocols ensure that users are who they claim to be. Examples include:

- **CHAP**: Challenges user with a nonce.
- **Kerberos**: Uses tickets and time-based validation.
- **OAuth**: Delegates user access securely.
  They are crucial to prevent impersonation, unauthorized access, and session hijacking.

◇ Scenario-Based Case Study

Scenario:
An IT firm is experiencing frequent unauthorized access attempts to their confidential design files. Their current system uses simple password-based login and folder-based permissions. They wish to improve access control and authentication.

Question 1: Identify and explain two major flaws in their existing system.
Answer:

1. **Weak user authentication** – Passwords alone are insufficient against modern attacks like phishing.
2. **Ineffective access control** – Folder-based permissions do not scale or adapt to user behavior/context.

Question 2: Recommend a combination of RBAC and ABAC to secure access.
Answer:
Implement RBAC to define broad roles: ‘Designer’, ‘Manager’, ‘Contractor’. Use ABAC to enforce fine-grained policies: ‘Designers can access files only from office IP during working hours’, or ‘Contractors cannot access confidential folders regardless of role’.

Question 3: Suggest an authentication protocol better than simple passwords. Why?
Answer:
Use two-factor authentication (2FA) or implement OAuth with token-based validation. These provide stronger protection by requiring more than just a password.

Question 4: How can Attribute-Based Encryption enhance their information storage?
Answer:
Encrypt files based on attributes like user role, department, or clearance level.

Only users with matching attributes can decrypt the data, adding an extra layer of security even if the storage is compromised.