Here are **10 multiple-choice questions (MCQs)** based on the topics from **Module 2: Authentication and Access Control**, each with its **correct answer and explanation**:

---

1. Which of the following best defines authentication?

A) Ensuring data is encrypted before storage
B) Verifying the identity of a user or system
C) Controlling access based on user roles
D) Encrypting data during transmission

✅ **Answer: B**
Explanation: Authentication is the process of verifying the identity of a user, device, or system before allowing access.

---

2. In symmetric key management, which of the following is true?

A) A unique public key is used by each party
B) The same key is used for both encryption and decryption
C) Keys are only used for signing documents
D) Key management is not required

✅ **Answer: B**
Explanation: Symmetric key encryption uses the same key for both encryption and decryption, making secure key exchange critical.

---

3. What is a main feature of hierarchical key management?

A) Each user has a randomly generated key
B) Keys are unrelated to each other
C) Keys are organized in a layered structure for scalability
D) It is used only for wireless networks

✅ **Answer: C**
Explanation: Hierarchical key management structures keys in a

layered manner, allowing better scalability and simplified key distribution.

---

4. Which of the following is an international standard for information security management systems (ISMS)?

A) IEEE 802.11
B) ISO/IEC 27001
C) WEP
D) RSA

✓ **Answer: B**
Explanation: ISO/IEC 27001 is a globally recognized standard for managing information security.

---

5. Which protocol is commonly used for secure user authentication over a network?

A) FTP
B) HTTP
C) Kerberos
D) Telnet

✓ **Answer: C**
Explanation: Kerberos is a network authentication protocol that uses tickets to allow nodes to communicate securely.

---

6. Which access control technique checks user credentials before granting entry to a system?

A) Logging
B) Authorization
C) Access control list (ACL)
D) Authentication

✓ **Answer: D**
Explanation: Authentication checks the identity of the user before access is allowed.

7. In which access control model are permissions directly assigned to users?

A) Discretionary Access Control (DAC)
B) Role-Based Access Control (RBAC)
C) Attribute-Based Access Control (ABAC)
D) Mandatory Access Control (MAC)

✅ **Answer: A**
Explanation: DAC allows the data owner to assign permissions directly to specific users.

8. What is a key benefit of Role-Based Access Control (RBAC)?

A) It provides encryption keys for data storage
B) It grants access based on attributes of users
C) It simplifies management by assigning permissions to roles rather than individuals
D) It prevents any access to data

✅ **Answer: C**
Explanation: RBAC improves manageability by assigning permissions to roles, and users are assigned roles.

9. Attribute-Based Access Control (ABAC) differs from RBAC by:

A) Using fixed permissions for each role
B) Basing access decisions on policies that evaluate user, resource, and environment attributes
C) Requiring biometric authentication only
D) Encrypting attributes

✅ **Answer: B**
Explanation: ABAC uses policies to make dynamic access decisions based on multiple attributes.

10. What is the purpose of physical access controls in information security?

A) Encrypting stored data
B) Securing access to logical systems only
C) Preventing unauthorized physical access to systems and data
D) Blocking phishing attacks

✅ **Answer: C**
Explanation: Physical access controls protect physical infrastructure (e.g., server rooms) from unauthorized entry.

Here are **10 more MCQs (numbered 11 to 20)** based on **Authentication and Access Control** topics:

---

11. Which of the following is NOT a method of user authentication?

A) Password
B) Biometric fingerprint
C) Username
D) Smart card

✅ **Answer: C**
Explanation: A username identifies the user but does not verify their identity. Authentication methods include password, biometrics, and smart cards.

---

12. Which key management scheme involves a trusted third party for key distribution?

A) Peer-to-peer key exchange
B) Public Key Infrastructure (PKI)
C) Static key system
D) Manual key sharing

✅ **Answer: B**
Explanation: PKI uses a Certificate Authority (trusted third party) to issue and manage digital certificates and keys.

---

13. Which access control model is the strictest and based on security labels and clearances?

A) DAC
B) RBAC
C) MAC
D) ABAC

✅ **Answer: C**
Explanation: Mandatory Access Control (MAC) restricts access based on security clearances and classifications.

---

14. What is the main component of an Access Control List (ACL)?

A) Encryption algorithm
B) List of users and their associated permissions
C) User passwords
D) Public keys

✅ **Answer: B**
Explanation: An ACL defines which users or system processes can access objects and what operations they can perform.

---

15. In Attribute-Based Encryption (ABE), access is granted based on:

A) Role hierarchy
B) Fixed policies only
C) Matching attributes between user and ciphertext policy
D) A single master key

✅ **Answer: C**
Explanation: ABE grants access if the user's attributes match the access structure embedded in the encrypted data.

---

16. Which of the following is a disadvantage of RBAC?

A) Easy scalability
B) Difficult to manage dynamic or contextual access needs
C) Simplified permission assignment
D) Useful for large organizations

✅ **Answer: B**
Explanation: RBAC struggles with dynamic or context-based access scenarios (like time-based or location-based access), which ABAC handles better.

---

17. What is the purpose of two-factor authentication (2FA)?

A) To avoid the use of passwords
B) To encrypt user passwords
C) To use two different forms of identification for higher security
D) To disable access temporarily

✅ **Answer: C**
Explanation: 2FA increases security by requiring two distinct types of authentication (e.g., password + OTP).

---

18. In key management, what is key revocation?

A) Encrypting a key
B) Backing up a key
C) Withdrawing a key’s validity due to compromise or expiration
D) Publishing a new key

✅ **Answer: C**
Explanation: Key revocation is the process of rendering a key invalid, usually due to security breaches or expiration.

---

19. Which of the following physical control prevents tailgating into secure areas?

A) Biometric scanner
B) Surveillance camera
C) Turnstile or mantrap
D) Password authentication

✅ **Answer: C**
Explanation: Turnstiles or mantraps are physical controls that prevent unauthorized individuals from entering along with authorized users (tailgating).

---

20. What does a security token typically provide during user authentication?

A) Encryption algorithm
B) Time-based or event-based OTP (One-Time Password)
C) Biometric scan
D) User's full credentials

✅ **Answer: B**
Explanation: Security tokens often generate OTPs to be used as part of multi-factor authentication.

Let me know if you'd like a combined PDF/CSV/JSON of these 20 MCQs or want more question sets!