**1.**

**(A)**

**i.**

**Message authentication using One-Way Hash function**

* **Using symmetric encryption** 
  + Message is hashed by using Hash function(H),and hashed result encrypted with a symmetric key (K).and Message with the encrypted hash to Destination B, In the destination B, message with encrypted hash use hash function produce a result(result1) for comparison, message with encrypted hash decrypted by symmetric key (K) produce result2,and compare result1 and result2 whether same.
* **Using public-key encryption** 
  + Message is hashed by using Hash function(H) to produce a hash, hash encrypted with sender’s private key(PRa), The message with encrypted hash send to Destination B message with encrypted hash use hash function produce a result(result1) for comparison, message with encrypted hash decrypted by sender’s public key (Pua) produce result2,and compare result1 and result2 whether same.
* **Using secret value** 
  + Message combined with secret value(K),and the combination is hashed by hash function(H)The hash is sent along with the message to the destination B,

In the destination B, message combined with same secret value(K) and hashed, after that compare with the hash we received

**ii.**

I think scheme a is less costly computationally, because scheme a is symmetric encryption, they use the same key for encryption and decryption, compare to public-key, computational cost relatively low.

**(B)**

I think Elliptic curve cryptography(ECC) is more suitable, ECC have the same security level as RSA, but with much smaller keys (faster computation and reduce resource usage)

**(C)**

**i.**

Digital Envelopes consist of two steps of encryption: use random symmetric key encrypted and use receiver’s public key to encrypt random symmetric key, and encrypted symmetric key just only decrypted by receiver’s private key. The other key cannot decrypt it.

**ii.**

* confidentiality
* Integrity
* authentically

**(D)**

* **Access control:**
  + Ensure that just only authorized user and system can access or modify the stored data.
* **Encryption:**
  + Use AES to encrypted data stored.
* **Backup and recovery**:
  + Implement regular data backup to ensure that data can be recovered in the event of data loss or corruption.

**2.**

**(A)**

**ABAC(Attribute Based Access Control)** used to enforce Database Security based on Subject Attributes(e.g. Name, clearance), Object Attributes(e.g. Type, classification) and Environment Attributes(e.g. time temperature) to control to access database.and according to Access Control Polices to judge this user whether visit database, For example, a company called ‘Apple’, The Access Control Polices may be state Software manger just only access database in the company and on working hours. He can’t access database in somewhere other than company and not in working hours.

**(B)**

An attacker embed malicious SQL code fragments in the cookie such that when the application server builds an SQL query based on the cookie’s content, the structure based on that cookie is already modified.

Attacker may be through client-side scripts, the modified cookie contains malevolent SQL commands, when user access application, the server reads the cookie and use that SQL command to construct database queries.

**(C)**

**SQLi attacks covered The Computer Misuse Act 1990**

* **Section 1** – causing a computer to perform a function with intent to secure unauthorized access to computer material SQL injection can be seen as an attempt to gain unauthorized access to data in the database.
* **Section 2** – unauthorized access with intent to commit or facilitate commission of further offence . SQL injection attack could be used as commit further crimes, like data theft or fraud.

**(D)**

Plan-Do-Check-Act process mode consist of four part: Plan, Do, Check, Act

* **Plan**: build a security policy addresses the purpose , IT security requirements , risk management approach
* **Do**: Implement Security policy, include security awareness and training and integration of security into systems development
* **Check**: Conduct regular security reviews to assess the effectiveness of the security measures implemented.
* **Act**: Make necessary adjustments or improvements to security policies and controls based on the insights gained from the "check" phase. This may involve updating policies.