Question 1

Network structure:

The sender A wants to send a message securely to receiver B through a sequence of mix nodes: M1 → M2 →M3 → M4. Each mix will decrypt only one layer of encryption and will forward the message to the next hop (onion encryption)

The Keys:

First, the sender A receives the public keys of all mixes:
For M1 → PK (1)
For M2 → PK (2)
For M3 → PK (3)
For M4 → PK (4)

Only the specific mix knows it corresponding private key:
M1 knows →SK (1)
M2 knows →SK (2)
M3 knows →SK (3)
M4 knows →SK (4)

The sender A will use these keys to build the encryption like an onion. The innermost layer is meant for M4, then wrapped for M3, then wrapped for M2 and then lastly wrapped for M.

The Onion Encrypted Message:

We will say that m is the massage that sender A wants to send to recipient B.
We will say that Encryption_PK(n) is the function which will encrytpt based on the public key of mix M(n)

The message sent by A will look something like this:

```
Encryption_PK(1)(
        ADDRESS = M(2) ||
        Encryption_PK(2)(
                        Adress = M3 ||
                        Encryption_PK3(
                                        Adress=M4 ||
                                        Encryption_PK4(
                                                Adress = B ||
                                                M
                                                        ))))
```

In this encryption:

1. M1 decrypts with SK(1) → see M2's address →forwards the rest
2. M2 decrypts with SK(2) →see M3's address → forwards the rest
3. Only M4 sees the final destination, B and the message

Question 2

Unlinkability is the the property which ensures that an observer can not dettermine whether 2 or more items of “interest” like: messages ,actions or sessions originae from the same user.

Unlinkability is different from anonymity because anonymity only ensures that a single action or message cannot be tracked back to a specific identity. Anonymity only protects identity in one instance while unlinkability protects it in multiple instances or cases.

Unlinkabiltiy is critical because even if each individual intereaction is anonymous, an attacker could correlate multiple actions to build a user profile or reveal identy over time if those actions are linkable.

Question 3

In a mix network, message reordering prevents an observer from linking incoming message to outgoing ones based on order, breaking timing correlations.

Padding in a mix network ensures thaet all messages are in the same size, preventing size based correlation between senders and recievers.

Onion routing relies primarily on multiple layers of encryption to conceal the path of the message thorugh the network. Each code decrypts one layer to reveal the next hope but messages typically maintain order and way vary in size. This is why onion routing protects against content and path disclosure but provides weaker protection against traffic analysis compared to mix networks.