1. While determining the public RSA key, Bob needs to select p, q, and e.
Justify which of these must be chosen randomly. (4 points)

> p, q has to be chosen randomly.
>
> Because if p, q are chosen randomly, n, d and y will not be a fixed value or easy to predict.
>
> If e is fixed, as n and d is unknown, it is hard to compute the y and d. But if either p or q is fixed, the complexity of the attack will largely decrease, as the space will shrink from n^2 to n when computing n.

2. Explain why Diffie-Hellman is subject to the Man-in-the-Middle attack. (3 points)

> If the attacker captures the key exchange message sent from A, then the attacker can disguise himself as B, then set a connection with A using his own private key. Then sends a key exchange message to B, and set a connection with B. Therefore, the attacker will receive messages from A and B changing messages or do nothing, and none of them will be aware of it.

3. What is the advantage of using Merkle Puzzle for key exchange in comparison with other asymmetric key exchange protocols such as Diffie-Hellman key exchange? (3 points)

> Merkle Puzzle is resistant to the Man-in-the-Middle attack, which is somehow more secure than the Diffie-Hellaman key exchange.