1. Why should the same k value not be used multiple times in ElGamal encryption? (3 points)

> This is not CPA secure.
>
> For the ElGamal encryption described in the slice, when k is reused, c is fixed and c is the same if encrypting the same message. Hence, it is not secure.

2. How does RSA encryption achieve the property of confidentiality in electronic communication, and what is the role of the trapdoor function in this process? (3 points)

> RSA encryption uses RSA to replace the trapdoor function. Basically, RSA uses modulo calculation to achieve the property that the trapdoor function is easy to compute in one direction but difficult to compute in the reverse direction. And RSA is public-key cryptography, which makes its confidentiality.
>
> The trapdoor function here is to encrypt and decrypt the element for generating the key k.

3. What is the purpose of a digital signature, and how does it provide non-repudiation in electronic communication? (4 points)

> The digital signature is to make sure the integrity of the message sent from a public-key encryption scheme.
>
> It provides non-repudiation by a third party called certification authority. The certification authority verifies the parties, then the receiver can ask CA to make sure the message is from the authenticated sender.