Homework 6 (Zero-Knowledge Proofs)

Please submit your solutions to the email address 7ccsmsen at gmail dot com. Please submit only ASCII text or PDFs. Every solution should be preceded by the corresponding question, like:

Qn**:**	**…a difficult question from me…**
A:	**…an answer from you …**
Q$n+1$	**…another difficult question…**
A:	**…another brilliant answer from you…**

Solutions will only be accepted until 30th December!

1. Zero-knowledge protocols depend on three main properties called completeness, soundness and zero-knowledge. Explain what they mean?
2. Why do zero-knowledge protocols require an NP-problem as building block?
3. Why is it a good choice in a ZKP to flip a coin when requesting a proof from the person who knows the secret?