Homework 6

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?