

Homework 6 (Zero-Knowledge Proofs)

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

Q_n: ...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. Explain briefly the purpose of the certification authority in the public-private key encryption scheme.
2. Explain briefly what is meant by a certification authority becoming “too big to fail” when it has issued a large number of certificates.
3. In which situations does it make sense to install invalid (self-signed) certificates?
4. Zero-knowledge protocols depend on three main properties called completeness, soundness and zero-knowledge. Explain what they mean?
5. Why do zero-knowledge protocols require an NP-problem as building block?
6. Why is it a good choice in a ZKP to flip a coin when requesting a proof from the person who knows the secret?