22

Proofs and algorithms

“Let’s not try to define knowledge, but try to define zero-knowledge.”, Shafi Goldwasser.

Proofs have captured human imagination for thousands of years, ever since the publication of Euclid’s Elements, a book second only to the bible in the number of editions printed.

Plan:

- Proofs and algorithms
- Interactive proofs
- Zero knowledge proofs
- Propositions as types, Coq and other proof assistants.

22.1 EXERCISES

22.2 BIBLIOGRAPHICAL NOTES