

Description of Project Assignment

Proposal due: Tuesday, October 5, 2004.

A programming project can be the implementation of some cryptographic protocols, or using cryptographic protocols to achieve other objectives.

Possible topics include but are not limited to:

- Zero-knowledge proof
- Secure auction
- Fair exchange
- Threshold cryptography protocols
- Electronic cash
- Electronic voting systems
- File encryption
- Secure chat
- Secure card playing over the net

Students can work alone or in pairs. Each team will get one grade on the project.

Students are encouraged to discuss, either by emails or face-to-face meetings, with either the instructor and/or the TA about project ideas.

The proposal should be 1-4 pages, including references. It should include team members, expected outcome, plan, and references. It won't be graded. Feedbacks about the plan and the references will be given by the instructor about the proposal.