

Hard Problems in Cryptography — Colloquium

[Insert dates / term]

Meetings: [Day, time] · [Room] / Zoom: [link]

Organizer: [Your name] ([Email])

Sign-up: [Sign-up link]

Deadline: [Sign-up deadline]

Notes/Repo: [Shared notes link]

Overview

A weekly, participant-led colloquium on the computational problems that support modern cryptography and post-quantum designs. Each session pairs a short talk with a working discussion: we focus on precise problem statements, the core ideas behind major attacks, and what drives parameter choices.

Who it's for

Masters / advanced undergrad; PhD welcome. Comfort with modular arithmetic, basic linear algebra, and proof writing is enough. A short preliminaries handout will be provided.

Format (90 minutes)

- **Talk (30–40 min)** — rotating presenters, with a shared template
- **Working session (35–45 min)** — proof sketches + toy instances + attack walk-throughs
- **Discussion (10–15 min)** — assumptions, sharp edges, and open questions

Planned themes

Integer factorization (RSA/Rabin), discrete logarithms (finite fields and elliptic curves), lattices (SVP/CVP, SIS/LWE), code-based decoding (ISD), isogenies, multivariate quadratic systems (MQ), and hash-function security (collision/preimage, Merkle–Damgård/HMAC, quantum impact).

Participation

Presenting is encouraged but optional. Presenters will receive a lightweight checklist (definition + one reduction/equivalence + one attack mechanism + two practice problems). Everyone contributes questions in advance and helps maintain a clean shared set of notes.

Note. This is an educational research-reading group. We focus on publicly documented algorithms and standard security models.