Hard Problems in Cryptography Colloquium

[Insert Term / Date Range]

Meetings: [Day, Time] @ [Room] / Zoom: [Link]
Organizer: [Your Name] | **Contact: [Email]**
Sign-up: [Sign-up link / form] | **Deadline: [Sign-up deadline]**
Shared notes/repo: [Shared notes link]

What is this?
A structured, discussion-driven study group on the *hard computational problems* that underpin classical and post-quantum cryptography. Each week features a short talk by a participant followed by a guided board session (proof sketch + toy attack + Q&A).

Topics (tentative):

- Integer factorization (RSA/Rabin): ECM, QS, GNFS, Shor overview
- Discrete logarithms (finite fields & elliptic curves): Pollard ρ, Pohlig–Hellman, index calculus, pairing pitfalls
- Lattices (SVP/CVP, SIS/LWE): LLL/BKZ intuition; primal/dual/hybrid attacks
- Codes (syndrome decoding): McEliece context; ISD (Prange $\rightarrow$ BJMM)
- Isogenies: supersingular graphs; CSIDH-style actions; attack heuristics
- Multivariate (MQ): Gröbner/XL/hybrid; structural pitfalls
- Hash: CR/SPR/OW games; birthday bound; length extension; HMAC; quantum impacts

Audience / prerequisites
Masters/advanced undergrad; PhD welcome. You should be comfortable with modular arithmetic, basic linear algebra, and proof writing. We will share a short preliminaries handout.

Format (90 minutes/week)

- 30–40 min participant talk (rotating presenters)
- 30–40 min board session (practice problems / proof sketches)
- 10–15 min research-style discussion (assumptions, best-known attacks, open questions)

Why join?

- Build a coherent map of cryptographic hardness assumptions and their best-known attacks.
- Improve paper-reading and presentation skills in a supportive setting.
- Leave with a shared set of clean notes, a glossary, and a curated reference list.

How to participate
Sign up by **[Sign-up deadline]** using **[Sign-up link / form]**. Indicate whether you can present (recommended but optional). Presenters will get a template (definition + reduction + attack mechanism + 2 practice problems).

Note: This is an educational colloquium. We focus on publicly documented algorithms/attacks and do not discuss wrongdoing or misuse.