Hard Problems in Cryptography — Course Syllabus

[Insert Term, Year]

Course Information

Course Title:	Hard Problems in Cryptography
Term:	**[Insert Term, Year]**
Meeting Time/Place:	**[Insert Days/Times/Room]**
Instructor:	**[Insert Instructor Name]**
Email:	**[Insert Email]**
Office Hours:	**[Insert Office Hours / Location]**
Course Website:	**[Insert Course Website/LMS Link]**
Prerequisites:	**[Insert prerequisite statement]**

Catalog Description

This course studies the mathematical foundations and cryptanalytic landscape of core *hard problems* that underpin modern public-key and post-quantum cryptography. Topics include integer factorization, discrete logarithms in finite fields and elliptic curves, lattice problems (SVP/CVP, SIS/LWE), code-based syndrome decoding, isogenies of elliptic curves, multivariate quadratic systems (MQ), and cryptographic hash functions. For each family, we emphasize (i) formal problem definitions, (ii) standard reductions and security notions, (iii) best-known classical and quantum attacks, and (iv) parameter-selection principles and failure modes.

Learning Outcomes

By the end of the course, students will be able to:

1. State formal definitions of canonical hard problems (search/decision/distinguishing) used in cryptography.

2. Explain how cryptosystems reduce to these hard problems and articulate the assumptions involved.

3. Describe and analyze best-known attacks (classical and quantum), including when special structure invalidates generic security claims.

4. Perform back-of-the-envelope security estimates from asymptotic and heuristic complexity models (e.g., $\tilde{O}(\sqrt{n})$, $L_N[\alpha, c]$, $2^{\Theta(d)}$).

5. Critically evaluate parameter choices and identify common implementation pitfalls (subgroup validation, side channels, randomness failures).

6. Communicate cryptographic hardness arguments clearly in mathematically precise language.

Course Format and Levels

The course is designed for a mixed audience (upper-undergraduate, masters, PhD). Core lectures target the common baseline. Assignments are tiered:

- **UG track:** computation and conceptual mastery; small worked examples; short proofs.
- **MS track:** reductions, algorithmic analysis, and formal security games.
- **PhD track:** deeper proof obligations, modeling assumptions, and critique/comparison of attacks and parameter regimes.

Students may switch tracks with instructor approval.

Prerequisites

Recommended background:

- Discrete mathematics and proof writing (sets, functions, modular arithmetic).
- Linear algebra (vector spaces, matrices, rank/nullspace).
- Basic probability (conditional probability; expectation).
- Helpful: abstract algebra (groups, rings, fields), algorithms/complexity.

A brief review of required algebra and probability will be provided in Week 0 materials.

Texts and References

Primary references (free/standard):

- D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography* (online draft).
- J. Katz and Y. Lindell, *Introduction to Modern Cryptography* (security definitions).

Topic references (selected):

- H. Cohen, *A Course in Computational Algebraic Number Theory* (factoring background).
- L. C. Washington, *Elliptic Curves: Number Theory and Cryptography* (EC/DLP/isogenies background).
- D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems* (lattices).
- F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (codes).
- Cox–Little–O'Shea, *Ideals, Varieties, and Algorithms* (Gröbner bases, MQ).
- M. Bellare, R. Canetti, H. Krawczyk (HMAC) and hash-function design notes (hash).

Assessment and Grading

Weekly worksheets (tiered)	25%
Problem sets (biweekly; tiered)	25%
In-class quizzes (best $N-1$)	10%
Midterm (take-home or in-class)	15%
Final project (paper + short presentation)	25%

Final project. Students will complete either (i) a survey-style exposition of one hard-problem family and its attacks, or (ii) a small computational experiment (e.g., toy LWE attack comparison, ISD implementation on small codes), with a written report (6–10 pages MS/PhD; 4–6 pages UG) and a 8–12 minute presentation.

Assignments, Collaboration, and Academic Integrity

- **Collaboration:** Discussion is encouraged. Unless explicitly allowed, submitted solutions must be written independently.
- **Citation policy:** Any external sources (papers, code, notes, AI tools) must be cited. Include a brief "Resources Used" section.
- **Late policy:** [**Insert policy**] (e.g., 2 grace days total; otherwise 10% per day).
- **AI tools:** Allowed for brainstorming and checking, but all final writing must be your own; must cite use.

Accessibility and Student Support

Students requiring accommodations should contact [**Insert office**] and inform the instructor as early as possible. The course aims to provide inclusive access to materials and assessments.

Course Schedule (Tentative)

Week	**Topic**	**Key Concepts / Hard Problems**	**Deliverables**
0	Preliminaries	Security parameter; PPT/negligible; search vs decision vs distinguishing; L-notation; basic group/field review	Diagnostic / setup

Continued on next page

Week	Topic	Key Concepts / Hard Problems	Deliverables
1	Integer Factorization	RSA/Rabin context; $\varphi(N)$ and order-finding reductions; ECM, QS, GNFS; Shor overview	Worksheet 1
2	Discrete Logarithms	DLP/CDH/DDH; BSGS/Pollard; Pohlig–Hellman; index calculus/NFS-DL; ECDLP vs finite fields; Shor	Worksheet 2; Quiz 1
3	Lattices I	Lattices, duals, determinant; Minkowski; SVP/CVP; LLL/BKZ overview	Worksheet 3
4	Lattices II + Codes intro	SIS/LWE formalism; primal/dual/hybrid/BKW attacks; syndrome decoding and SD	PS 1 due
5	Codes	McEliece context; ISD (Prange → BJMM); structural attacks; quantum notes	Worksheet 4; Quiz 2
6	Isogenies	EC basics; isogenies, kernels, Vélu (concept); supersingular graphs; CSIDH-style actions; protocol-specific breaks; quantum hidden shift	Worksheet 5
7	Multivariate (MQ)	MQ definition; Gröbner (F4/F5); XL/hybrid; MinRank/rank attacks; scheme pitfalls	PS 2 due
8	Hash functions	CR/SPR/OW games; birthday bound; Merkle–Damgård, length extension; HMAC; quantum Grover impacts	Worksheet 6; Quiz 3
9	Cross-cutting security	Comparing attack models; parameter selection; implementation pitfalls; case studies (NIST PQC overview optional)	Worksheet 7
10	Project week	Student presentations; synthesis and review	Final report + presentation

Course Policies (Template)

Communication: Course announcements will be posted on [**Insert Course Website/LMS Link**]. Students are responsible for checking regularly.

Regrades: [**Insert policy**] (e.g., within 7 days; include a written explanation).

Recording: [**Insert policy**].

Changes: The instructor may modify the schedule in response to pacing and feedback.