# Course Proposal:
# CMSC 65x: Introduction to Cryptography

Jonathan Katz

**Catalog description:**
**CMSC 65x, Introduction to Cryptography (3)** Prerequisite: CMSC451 or CMSC452 or CMSC456.
Graduate-level introduction to modern cryptography. Topics include symmetric-key encryption, hash functions, message-authentication codes, block-cipher design, theoretical foundations, number theory, public-key encryption, and digital signatures.

**Motivation and background.** Cryptography is a core part of cybersecurity as well as a central topic in theoretical computer science. Most other top-tier schools regularly teach graduate cryptography courses. Cryptography courses at UMD have tended to be very popular: Three sections of CMSC 456 (undergraduate cryptography) are offered each academic year, and my current offering of graduate cryptography has 26 students from computer science, electrical engineering, mathematics, and physics. A graduate-level *Introduction to Cryptography* course (listed as CMSC 858K) has been taught three times, roughly once every 4 years, and I believe there would be sufficient demand from the students to teach it more frequently. Student demand is likely to increase with the growth of the Maryland Cybersecurity Center.

**Course description.** The course is intended to provide students with a broad introduction to modern cryptography, suitable both for students intending to pursue research in the area as well as those who may use cryptography as part of their research in another field (e.g., networking or security). Mathematical maturity is assumed, but no prior exposure to cryptography is expected. Because of this, the topics covered are very similar to those taught in the undergraduate cryptography course (CMSC 456); however, in the graduate course the topics are covered more rigorously, in more depth, and at a faster pace; advanced topics are included as well.

**Textbooks.** I have used the textbook I co-authored (J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC Press, 2007) the last two times I taught the class. Before that, I did not use any textbook.

**Syllabus.** The following syllabus reflects what was taught in Spring 2011, but there is flexibility in some of the topics covered, especially toward the end.

- **Introduction and perfect security** (2 lectures). Overview. Historical encryption schemes and the modern approach. Unconditional secrecy (Shannon security) and its limitations.
- **Symmetric-key encryption** (3 lectures). Computational security; formal definitions and proofs by reduction; notions of security for symmetric-key encryption and relations among them. Pseudorandom generators and pseudorandom functions (block ciphers). Constructing secure encryption schemes; modes of encryption. Security against chosen-ciphertext attacks.

- **Message authentication** (3 lectures). Integrity vs. secrecy, and the importance of message authentication. Collision-resistant hash functions and methods for their construction. Birthday attacks. CBC-MAC and HMAC. Achieving simultaneous privacy and message integrity.

- **Theoretical foundations** (4 lectures). One-way functions and (conjectures) examples. The Goldreich-Levin theorem. Constructing pseudorandom generators from one-way permutations; increasing the expansion of a pseudorandom generator. Building pseudorandom functions from pseudorandom generators. Feistel networks, and converting pseudorandom functions to pseudorandom permutations.

- **Number theory and algebra** (5 lectures). Basic (algorithmic) number theory and group theory. Primality testing. The factoring assumption and the RSA problem. Cyclic groups, the discrete logarithm problem, and the Diffie-Hellman problems. One-way permutations from number-theoretic problems.

- **Public-key encryption** (4 lectures). The public-key setting, and advantages relative to the symmetric-key setting. Diffie-Hellman key exchange. Notions of security for public-key encryption and relations among them. The "textbook RSA" encryption scheme, and why it is insecure. Padded RSA encryption; El Gamal encryption. Hybrid encryption. Trapdoor permutations, and their use in constructing encryption schemes. Trapdoor permutations based on RSA or the factoring assumption. Security against chosen-ciphertext attacks.

- **Digital signatures** (2 lectures). Introduction, definitions, and comparison to message authentication codes. The "textbook RSA" signature scheme, and why it is insecure. The digital signature standard. The hash-and-sign paradigm. The Lamport one-time signature scheme. Signature schemes from one-way functions.

- **The random oracle model** (2 lectures). Overview of the random oracle model; pros and cons. Constructing public-key encryption schemes and digital signatures in the random oracle model.

- **Advanced topics** (4 lectures). Topics may include: identification schemes and the Fiat-Shamir transform, efficient constructions of CCA-secure encryption schemes; zero-knowledge proofs; introduction to secure computation.