

Table of Contents

Overview and Usage Guide	ix
Mini-Courses	xiii
Acknowledgments	xv
Preliminaries	3
Introduction of some basic notation that is used in all subsequent lectures. Review of some computational complexity classes. Description of some useful probability facts.	
Lecture 1	13
Introduction to private key cryptosystems, pseudorandom generators, one-way functions. Introduction of some specific conjectured one-way functions.	
Lecture 2	21
Discussions of security issues associated with the computing environment of a party, including the security parameter of a protocol. Definition of an adversary, the achievement ratio of an adversary for a protocol, and the security of a protocol. Definitions of one-way functions and one-way permutations, and cryptographic reduction.	
Lecture 3	35
Definition of a weak one-way function. Reduction from a weak one-way function to a one-way function. More efficient security preserving reductions from a weak one-way permutation to a one-way permutation.	
Lecture 4	49
Proof that the discrete log problem is either a one-way permutation or not even weak one-way permutation via random self-reducibility. Definition of a pseudorandom generator, the next bit test, and the proof that the two definitions are equivalent. Construction of a pseudorandom generator that stretches by a polynomial amount from a pseudorandom generator that stretches by one bit.	
Lecture 5	56
Introduction of a two part paradigm for derandomizing probabilistic algorithms. Two problems are used to exemplify this approach: witness	

sampling and vertex partitioning.

Lecture 6 64

Definition of inner product bit for a function and what it means to be a hidden bit. Description and proof of the Hidden Bit Theorem that shows the inner product bit is hidden for a one-way function.

Lecture 7 70

Definitions of statistical measures of distance between probability distributions and the analogous computational measures. Restatement of the Hidden Bit Theorem in these terms and application of this theorem to construct a pseudorandom generator from a one-way permutation. Description and proof of the Many Hidden Bits Theorem that shows many inner product bit are hidden for a one-way function.

Lecture 8 79

Definitions of various notions of statistical entropy, computational entropy and pseudoentropy generators. Definition of universal hash functions. Description and proof of the Smoothing Entropy Theorem.

Lecture 9 88

Reduction from a one-way one-to-one function to a pseudorandom generator using the Smoothing Entropy Theorem and the Hidden Bit Theorem. Reduction from a one-way regular function to a pseudorandom generator using the Smoothing Entropy Theorem and Many Hidden Bits Theorem.

Lecture 10 95

Definition of a false entropy generator. Construction and proof of a pseudorandom generator from a false entropy generator. Construction and proof of a false entropy generator from any one-way function in the non-uniform sense.

Lecture 11 105

Definition of a stream private key cryptosystem, definitions of several notions of security, including passive attack and chosen plaintext attack, and design of a stream private key cryptosystem that is secure against these attacks based on a pseudorandom generator.

Lecture 12 117

Definitions and motivation for a block cryptosystem and security against chosen plaintext attack. Definition and construction of a pseudorandom

function generator from a pseudorandom generator. Construction of a block private key cryptosystem secure against chosen plaintext attack based on a pseudorandom function generator.

Lecture 13 128

Discussion of the Data Encryption Standard. Definition of a pseudo-random invertible permutation generator and discussion of applications to the construction of a block private key cryptosystem secure against chosen plaintext attack. Construction of a perfect random permutation based on a perfect random function.

Lecture 14 138

Construction of a pseudorandom invertible permutation generator from a pseudorandom function generator. Definition and construction of a super pseudorandom invertible permutation generator. Applications to block private key cryptosystems.

Lecture 15 146

Definition of trapdoor one-way functions, specific examples, and construction of cryptosystems without initial communication using a private line.

Lecture 16 154

Definition and construction of a universal one-way hash function.

Lecture 17 162

Definition and construction of secure one bit and many bit signature schemes.

Lecture 18 174

Definition of interactive proofs **IP** and the zero knowledge restriction of this class **ZKIP**. Definition and construction of a hidden bit commitment scheme based on a one-way function. Construction of a **ZKIP** for all **NP** based on a hidden bit commitment scheme.

List of Exercises and Research Problems 185

List of Primary Results 195

Credits and History 199

References 211

Notation 221