Contents

UNIT I

The Cryptology Model, Random and Pseudorandom Keys, When Are Problems Hard? P, NP, and Feasibility, Randomization, BPP, and RP, Infeasibility and PP, P/poly, Polynomial size circuit, Function Ensembles, Pseudorandom Number Generators.

UNIT II

One way functions, One-way functions with public input, Pseudo-random number generators and one way functions, Weak one way functions, Converting Weak One Way Functions to One Way Functions, Reverse expansion, (Weak) One-way permutations, Square Root Extraction and Nontrivial Factoring Problems.

UNIT III

A Little Bit of Number Theory, Next-bit Unpredictability, Stretching the output of a pseudorandom number generator, Private Key Stream Cryptosystems, Simple Passive Attack, Simple Chosen Plaintext Attacks (Informal Definition), Simple chosen plaintext attack, Block cryptosystems.

UNIT IV

Pseudo random function generators, Trapdoor functions & RSA, Square Root Extraction, Existence of Pseudorandom Number Generators, Some Probability Review, Hidden Inner Product Bit, More on Hidden, Many Hidden Bits, Statistical Distinguishability of Distributions , Computational Indistinguishability of Distributions , Strengthening the Hidden-Bit Theorems ,A Version of the Triangle , Entropy and Information.

UNIT V

Prefix-free codes, Huffman codes, PRNG's from One-Way Functions , Hash Functions and One-Way Hash Functions , Applications of Hash Functions ,Thwarting the birthday attack ,Blinded signatures.

Texts / References

1. B. Schneider, *Applied Cryptography*, Wiley, 1996.
2. M. Luby, *Pseudorandomness and Cryptographic Applications*, Princeton U. Press, 1996.
3. A, Menezes, P. van Oorshot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
4. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1994.
5. O. Goldreich, *Foundations of Cryptography*, unpublished manuscript (available electronically at http ://www.eccc.uni-trier.de/eccc-local/ECCC-Books/oded book readme.html)

Mrs. Sheela for