



PURE MATHEMATICS 529
"ADVANCED CRYPTOGRAPHY AND CRYPTANALYSIS"

Calendar Description: H(3-0)

Probability and perfect secrecy. Provably secure cryptosystems. Prime generation and primality testing. Cryptanalysis of factoring based cryptosystems. Discrete log based and elliptic curve cryptography and cryptanalysis. Other advanced topics may include hyperelliptic curve cryptography, other factoring methods and other primality tests.

Prerequisite: Pure Mathematics 429.

Syllabus

Table with 2 columns: Topics and Number of Hours. Topics include Probability and Perfect Secrecy, Provably secure cryptosystems, Prime Generation and Primality Testing, Cryptanalysis of Factoring-Based Cryptosystems, Discrete Log Based Cryptography and Cryptanalysis, and Elliptic Curve Cryptography and Cryptanalysis. Total hours: 36.

\*\*\*\*\*