

PURE MATHEMATICS 519 "INFORMATION THEORY, CODES, AND CRYPTOGRAPHY"

Calendar Description: H(3-0)

A continuation of Pure Mathematics 419. Topics include Entropy, Shannon's Theorem, Hamming codes, Reed-Muller codes, Reed-Solomon codes, MDS codes and finite geometries, Ergodic and Markov processes.

Prerequisite: Pure Mathematics 419.

<u>Topics</u>	<u>Number of Hours</u>
Review of symmetric and asymmetric encryption.	3
Symmetric encryption and entropy	3
Shift registers	3
Source coding, Prefix codes, typical sequences	3
Data compression, Huffmand and Lempel Ziv	3
Conditional entropy, channel coding, signal to noise ratio	3
Stationary, ergodic and Markov sources	3
General codes, Hadamard matrices, Gilbert-Varshamov bound	3
Linear codes, syndrome decoding	3
Cyclic codes and shift registers	3
Reed-Solomon codes, the Berlekamp-Massey algorithm	3
MDS codes, introduction to convolutional codes	3
TOTAL:	36
