Secure Communications and Data Encryption
ELG 5373 (92.515O)
Course Outline

Jean-Yves Chouinard
School of Information Technology and Engineering
University of Ottawa
Email: chouinar@site.uottawa.ca
Web page: http://www.site.uottawa.ca/∼chouinar/

Lectures:	Monday	17:30 to 19:00	MRT 250 (Morisset Hall, 65 University)
	Wednesday	17:30 to 19:00	MNT 204 (Montpetit Hall, 125 University)

OCIECE Calendar Description:
Secure communications: encryption and decryption. Entropy, equivocation and unicity distance. Cryptanalysis and computational complexity. Substitution, transposition and product ciphers. Data Encryption Standard (DES): block and stream cipher modes. Modular arithmetics. Public key cryptosystems: RSA, knapsack. Factorization methods. Elliptic curve cryptography. Authentication methods and cryptographic protocols.

Prerequisites: ELG 5119 or 94.553 (Stochastic Processes) or equivalent.

Course evaluation scheme:	Assignments:	30%
	Term paper and presentation:	40%
	Final examination:	30%

Textbook: Course notes 2002