UNIVERSITY OF CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics

PURE MATHEMATICS 329
"INTRODUCTION TO CRYPTOGRAPHY"

Calendar Description: H(3-1T)

Description and analysis of cryptographic methods used in the authentication and protection of data. Classical cryptosystems and cryptanalysis, information theory and perfect security, the Data Encryption Standard (DES) and Public-key cryptosystems.

Prerequisite: Mathematics 271.

Proposed Syllabus

Topics	**Number of hours**
Basic ideas and definitions: basic definitions, requirements for cryptosystems, cryptanalysis	3
Classical cryptosystems: substitution ciphers, codes, n-gram encipherments, polyalphabetic ciphers, the ϕ-statistic, determining the number of alphabets, mixed polyalphabetic ciphers, cryptanalysis	8
Information theory: entropy, rate and redundancy, equivocation and perfect security, the one-time pad, unicity distance	6
Product ciphers and DES: transposition ciphers, product ciphers, the Data Encryption Standard (DES), strengths and weaknesses of DES, analytic attacks on DES	5
Taxonomy of Cryptosystems: modes of operation for block ciphers, stream ciphers, certified DES modes, authentication	2
Elementary number theory: some number theoretic algorithms, some number theoretic results	2
Public-key cryptography: one-way functions, public key cryptography (PKC), the RSA cryptosystem, security of RSA, authentication using PKC, applications of authentication, other applications of PKC	7
Elementary intractability theory: problems and complexity, NP-completeness, summary	3
TOTAL HOURS	**36**

* * * * * * *

2003:12:23
JL:jml