# Table of Contents: COMP4631


- Lecture 01: Course Introduction and Physical Security
- Lecture 02: Introduction to Computer Security
- Lecture 03: Mathematical Foundations I
- Lecture 04: Mathematical Foundations II
- Lecture 05: Introduction to Cryptography
- Lecture 06: One-key Block Ciphers
- Lecture 07: Several One-key Block Ciphers
- Lecture 08: Key Management for One-key Ciphers
- Lecture 09: Introduction to Public-Key Cryptography
- Lecture 10: The RSA Public-key Cipher
- Lecture 11: Public Key Infrastructure
- Lecture 12: Active Attacks and the Digital Signature Scheme

- Lecture 13: Hash Functions and Keyed Hash Functions
- Lecture 14: Several Security Protocols
- Lecture 15: The Kerberos Authentication Protocol
- Lecture 16: A Review of Major Security Primitives
- Lecture 17: Electronic Mail Security
- Lecture 18: Access Control
- Lecture 19: Identification and Authentication
- Lecture 20: Unix Security
- Lecture 21: Network Security: IP Security
- Lecture 22: Web Security: Secure Sockets Layer
- Lecture 23: Firewalls
- Lecture 24: Virtual Private Networks
- Lecture 25: Secure Shell
- Lecture 26: Denial of Service Attacks and Defences