COMP 4140 - Introduction to Cryptography and Cryptosystems

Calendar Description: Description and analysis of cryptographic methods used in the authentication and protection of data. Classical cryptosystems and cryptoanalysis, the Data Encryption Standard (DES) and Public-key cryptosystems.
Prerequisites: COMP 2130, Students must be registered in fourth year of a Major or Honours programme in the Department of Computer Science.

Outline

1) Basic Ideas and Definitions (1 week)
2) Classical cryptosystems (one-key) (3 weeks)
Shift cipher, Substitution ciphers, Affine Ciphers, Vigenere Cipher, Hill Cipher, Permutation Cipher, Stream Cipher,
3) Information Theory (2 ⅓ weeks)
Probability and one-time pads, Entropy and Unicity Distance, Product Ciphers
4) Block Ciphers (3 weeks)
Substitution and Permutation Networks, Differential Attack, AES
5) Public Key Cryptosystems (2/3 week)
Introduction and Number Theory, RSA, Failure of Protocols
6) Cryptographic Hash Functions (2 weeks)
Security of Hash Functions, Secure Hash Algorithm (SHA)

Text: D. R. Stinson, *Cryptography – Theory and Practice, Third Edition,* Chapman and Hall/CRC Boca Raton (2006)