

University of Pretoria Yearbook 2021

Information security 780 (ETH 780)

Qualification Postgraduate

Faculty [Faculty of Engineering, Built Environment and Information Technology](#)

Module credits 32.00

NQF Level 08

Prerequisites No prerequisites.

Contact time 32 contact hours per semester

Language of tuition Module is presented in English

Department Electrical, Electronic and Computer Engineering

Period of presentation Semester 1

Module content

Number theory: prime numbers, congruences, modular arithmetic, Euclid's algorithm, Fermat's theorem, Euler's theorem, Euler's phi-function. Block ciphers: Feistel cipher, DES, AES. Public key cryptography: RSA, Diffie-Hellman, digital signatures. Hash functions: MD 5, SHA-1, MAC, HMAC. Protocols: identification, authentication, key exchange, X.509. PGP, S/MIME, IPSec, SSL, VPN. Authentication protocols, key distribution, key management, random number generation.

The information published here is subject to change and may be amended after the publication of this information. The [General Regulations \(G Regulations\)](#) apply to all faculties of the University of Pretoria. It is expected of students to familiarise themselves well with these regulations as well as with the information contained in the [General Rules](#) section. Ignorance concerning these regulations and rules will not be accepted as an excuse for any transgression.