University of Pretoria Yearbook 2022

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 regulations and rules for the degrees published here are subject to change and may be amended after the publication of this information.

The General Academic Regulations (G Regulations) and General Student Rules apply to all faculties and registered students of the University, as well as all prospective students who have accepted an offer of a place at the University of Pretoria. On registering for a programme, the student bears the responsibility of ensuring that they familiarise themselves with the General Academic Regulations applicable to their registration, as well as the relevant faculty-specific and programme-specific regulations and information as stipulated in the relevant yearbook. Ignorance concerning these regulations will not be accepted as an excuse for any transgression, or basis for an exception to any of the aforementioned regulations.