Universiteit van Pretoria Jaarboek 2017

Informasiesekerheid 780 (ETH 780)

Kwalifikasie	Nagraads
Fakulteit	Fakulteit Ingenieurswese, Bou-omgewing en Inligtingtegnologie
Modulekrediete	32.00
Voorvereistes	Geen voorvereistes.
Kontaktyd	32 kontakure per semester
Onderrigtaal	Module word in Engels aangebied
Akademiese organisasie	Elektriese, Elektroniese en Re
Aanbiedingstydperk	Semester 1

Module-inhoud

*Hierdie inligting is slegs in Engels beskikbaar.

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.