

CYBERSÉCURITÉ (SEC)

SEC 5100 Fundamentals of Cybersecurity (3 units)

Security policies. Security mechanisms. Security awareness. User authentication. Applied Encryption. External and internal firewalls. Intrusion Detection, Security of operating systems, databases and software. Security of Web applications. Design of security system and components. Devices for security analysis: sniffers, attack detectors. Ethical issues in computer security.

Course Component: Lecture

Recommended prerequisite : It is recommended to have courses or practical experience equivalent to one of the following courses : CSI 3140, SEG 3102, CEG 3185. The courses CSI 4139, CEG 4799, SEC 5100 cannot be combined for units.

SEC 5101 Fundamentals of Cryptography (3 units)

The notion of secure communication. Building secure cryptosystems based on the assumption of computational hardness. Cryptographic one-way functions, trap-door functions, pseudorandom generators, and public/private-key encryption schemes. Computational indistinguishability and unpredictability. Digital signature and message authentication. Zero-knowledge/interactive proof systems. Application to e-commerce and e-trade.

Course Component: Lecture

Recommended prerequisite: It is recommended to have courses or practical experience equivalent to CSI 3105 and MAT 2377. The courses CSI 4108, SEC 5101 cannot be combined for units.