Protocols, cryptanalysis and mathematical cryptology

Titulaires
Olivier MARKOWITCH (Coordonnateur), Liran LERMAN et Christophe PETIT

Mnémonique du cours
INFO-F514

Crédits ECTS
5 crédits

Langue(s) d'enseignement
Anglais

Période du cours
Deuxième quadrimestre

Campus
Plaine

Contenu du cours

Secret Sharing. Oblivious transfer. Fair exchange protocols. Electronic commerce. Digital signatures.

Cryptanalyse différentielle et cryptanalyse linéaire.

Cryptographie par courbes elliptiques.

Générateurs aléatoires cryptographiquement robustes. Chiffrement sériel.

Algorithmes arithmétiques en cryptographie. Factorisation, tests de primalité, logarithme discret, génération de nombres premiers...

Méthodes originales : biométrie, cryptographie visuelle, cryptographie quantique...

Objectifs (et/ou acquis d'apprentissages spécifiques)

Initier aux méthodes et attitudes spécifiques en recherche en cryptologie.

Assimiler les principaux résultats de cryptanalyse moderne, notamment dans le design et l'analyse de primitives et de protocoles cryptographiques.

Analyser de façon critique quelques questions d'actualité du domaine.

Pré-requis et co-requis

Cours ayant celui-ci comme co-requis

INFO-Y099 | Multicore programming | 6 crédits

Méthodes d'enseignement et activités d'apprentissages

Exposé introductif, analyse et présentation interactive de résultats scientifiques, critique collective.

Contribution au profil d'enseignement

Acquérir des connaissances pointues dans son domaine, assimiler et maîtriser de nouveaux concepts, développer une démarche rigoureuse de raisonnement scientifique, élaborer un processus d'abstraction en vue d'une analyse et d'une démarche scientifiques, présenter oralement ou par écrit de manière claire, concise et rigoureuse les résultats d'un travail, développer une argumentation scientifique, résumer et synthétiser.

Références, bibliographie et lectures recommandées

Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography", Chapman & Hall.

Steven Galbraith, "Mathematics of Public Key Cryptography", Cambridge University Press.

Support(s) de cours

Université virtuelle

Autres renseignements

Lieu(x) d'enseignement

Plaine

Contact(s)

Christophe Petit- Département d'Informatique - Campus Plaine - CP212 - Bâtiment N/O, Bureau 2.N8.115 Email: christophe.petit@ulb.be

Olivier Markowitch - Département d'Informatique - Campus Plaine - CP212 - Bâtiment N/O, Bureau 2.N8.115A Email: olivier.markowitch@ulb.be

Méthode(s) d'évaluation

Projet

Construction de la note (en ce compris, la pondération des notes partielles)

Rapports de groupe et individuels; participation active au projet

Langue(s) d'évaluation principale(s)

Anglais

Programmes

Programmes proposant ce cours à la faculté des Sciences

MA-INFO | Master en sciences informatiques | finalité Spécialisée/bloc 1 et finalité Spécialisée/bloc 2 et MA-SECU | Master en cybersécurité | finalité Conception et Analyse de Systèmes/bloc 1 et finalité Stratégies en entreprise/bloc 1