Cryptologie et arithmétique

MHT633

Mention	**Mathématiques** **Parcours Mathématiques-informatique**	Semestre 6	6 ECTS

U.F.R. de Mathématiques et Informatique
Département de Mathématiques Pures
Enseignant référent : Michel Olivier (olivier@math.u-bordeaux1.fr) .
Pré-requis : MHT531, MHT532
Objectifs : étude descriptive des méthodes modernes de cryptographie basées sur l'arithmétique élémentaire.

	1	2	3	4	5	6	7	8	9	10	11	12	13
12 C(1h20) 1 DS	X	X	X	X	X	X	X DS	X	X	X	X	X	
24 TD(1h20)		X X	X X	X X	X X	X X	X X	X X	X X	X X	X X	X X	X X
2 DM				DM1						DM2			

Programme

- Description des systèmes cryptographiques anciens et cryptanalyse statistique
- Initiation à la théorie de Shannon
- Description de deux chiffrements symétriques modernes : DES et AES
- Les chiffrements asymétriques : RSA et logarithme discret
- Algorithmes de factorisation et tests de pseudo-primalité
- Des attaques du logarithme discret
- Signature, identification, échange de clefs : description de quelques protocoles

Modalités de contrôle des connaissances

Epreuves de la session 1	**Durées**	**Formule de calcul**
Examen	1h30 (EX1)	Max [EX1, (DS + 3 EX1)/4]
Contrôle continu : note du DS	1h20 (DS)	

Epreuves de la session 2	**Durées**	**Formule de calcul**
Examen	1h 30 (EX2)	Max [EX2, (DS+ 3 EX2)/4]