Initiation à la Cryptologie
MHT431

Mention	**Mathématiques** **Parcours Mathématiques et Informatique**	Semestre 4	6 ECTS

U.F.R. de Mathématiques et Informatique
Département de Mathématiques Pures
Enseignant référent : Michel Olivier (olivier@math.u-bordeaux1.fr) .
Pré-requis : MHT201.
Objectifs : acquisition des notions de base de la cryptologie. Description des fondements et des outils utilisés en cryptographie et cryptanalyse anciennes et modernes, symétriques et asymétriques.

	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	X DS	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

1. **Rappels d'arithmétique élémentaire.**
2. **Les chiffrements par décalage, substitution, Vigenère, permutation, affine, Hill, en chaîne.**
3. **Crypanalyse statistique des chiffrements mono-alphabétiques.**
4. **Crypanalyse des chiffrements poly-alphabétiques : test de Kasiski et indice de coïncidence.**
5. **Introduction aux LFSR (téléphonie cellulaire).**
6. **Le chiffrement symétrique DES.**
7. **Les chiffrements asymétriques : RSA et logarithme discret.**

Modalités de contrôle des connaissances

Epreuves	Durées	Coefficients
Examen	1h30	0.7
Devoir Surveillé	1h20	0.3
Session 2		
Examen	1h30	1.0