Cryptographie élémentaire

MHT203

Domaine	**Mention Mathématiques**	Semestre 2	3 ECTS

U.F.R. de Mathématiques et Informatique
Département de Mathématiques Pures
Enseignant référent : Michel Olivier (olivier@math.u-bordeaux1.fr) .
Pré-requis : MIS100.
Objectifs : initiation à la cryptographie, utilisation des statistiques sur le langage et utilisation de l'arithmétique élémentaire.

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

Programme

1. **Arithmétique élémentaire dans Z : congruences, division euclidienne, petit théorème de Fermat, algorithmes d'Euclide et de Bézout, équation ax=b modulo n, exponentiation binaire.**
2. **Les chiffrements anciens : décalage, substitution, Vigenère ; attaques statistiques.**
3. **La machine Enigma : description, nombre de clefs.**
4. **Les suites récurrentes linéaires et les LFSR.**
5. **Principe du chiffrement RSA.**

Modalités de contrôle des connaissances

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