Master Sciences et Technologies
Spécialité : Cryptologie et Sécurité Informatique

UE : Théorie de l'Information

Mention : Mathématiques ou Informatique **Semestre** 8 6 **ECTS**.

UFR : Mathématiques et Informatique **Département** : Mathématiques

Volume horaire :

24 heures de cours, 24 heures de TD.

Équipe pédagogique : Gilles Zémor (cours), Marie-Line Chabanol (TD).

Objectifs : Présenter les fondements de la théorie de Shannon en vue d'applications au codage correcteur, à la cryptographie, à la théorie du signal.

Programme :

- Entropie et information, entropie conditionnelle, information mutuelle.
- Codage de source, codage de Huffman, compression de Lempel-Ziv.
- Codage de canal, canaux discrets sans mémoire, notion de capacité, théorème de Shannon.
- Codes correcteurs, codes linéaires, matrice de parité, syndrôme, canal à effacements, canal binaire symétrique, codes élémentaires.
- Bornes sur les codes, codes aléatoires.
- Canaux «wire-tap», le problème de l'extraction d'aléa et l'amplification de secret, min-entropie, entropie de Renyi, familles universelles de fonctions de hachage.
- Les grandes familles de codes en blocs, codes cycliques, codes BCH, codes de Reed-Solomon, codes LDPC.

Modalités de contrôle des connaissances :

Épreuves	Durées	Coefficients
Examen	3h	2/3
DS	1h1/2	1/3