UE 2
SEMESTRE 4

SCI 4 Culture scientifique et traitement de l'information
SCI 460 Cryptographie (module complémentaire)

CM	TD	TP	Total
1,5	7,5	6	15

retour au module

retour au tableau S.1 - S.2

retour au tableau S.3 - S.4

OBJECTIFS COMPÉTENCES MINIMALES

Comprendre les concepts essentiels de cryptographie (chiffrement, déchiffrement, hachage, cryptographie à clé publique/privée, signature, zero-knowledge) ainsi que les protocoles et modes de fonctionnement usuels, qu'ils soient issus des web-services ou non.

PRÉ-REQUIS

Outils mathématiques pour l'informatique

CONTENU

Etude des protocoles élémentaires (SSL, TLS) ainsi que les algorithmes usuels rencontrés dans le domaine des services (Blowfish, E0, etc).

Plus généralement, il convient d'aborder les modes de protection des données, ainsi que les attaques existantes. Par ailleurs, les normes ainsi que les autorités de certification seront évoquées.

INDICATIONS DE MISE EN ŒUVRE

Etude du protocole https. Mise en place d'un htaccess afin de protéger une partie de site web.

MOTS-CLEFS

Chiffrement, déchiffrement, clé publique, clé privée, hachage, signature, SSL, TLS, autorités de certification.