Cryptographie

module complémentaire

DUT SRC – IUT d'Arles – 2010-2011

xavier.heurtebise@univ-provence.fr

http://x.heurtebise.free.fr

Objectifs de ce cours (PPN)

1. **Comprendre les concepts essentiels de cryptographie**
   - chiffrement et déchiffrement
   - hachage
   - cryptographie à clé publique/privée
   - signature
   - zero-knowledge

2. **Comprendre les protocoles et modes de fonctionnement**
   - étude des protocoles élémentaires (SSL, TLS, HTTPS)
   - algorithmes usuels rencontrés dans le domaine des services
   - modes de protection des données
   - attaques existantes
   - autorités de certification

Organisation du cours

- Le cours de cryptographie s'organise provisoirement en :

1. 2h de CM
2. 3h de TD
3. 5h de TP
4. 2 évaluations :
   a. Contrôle continu de 2h (coefficient 2)
   b. Compte rendu de TP (coefficient 1)

Total : 12h

Plan

1. **Introduction**
   - Terminologie
   - Mécanismes et services de sécurité
2. **Algorithmes de cryptographie**
   - Chiffrement simple
   - Chiffrement symétrique
   - Chiffrement asymétrique
3. **Intégrité et authentification**
   - Fonctions de hachage, scellement et signature
   - Authentification mutuelle et échange de clefs de session
   - Principe de certification
4. **Protocoles sécurisés**
5. **Législation française**
6. **Conclusion**