

NET4504 Sécurité des réseaux

Période : S8 / P2

ECTS : 4

Langue : Français

Organisation :

- Heures programmées / Charge Totale : 45/90
- Heures Cours/TD/TP/CF1 : 30/6/6/3

Objectifs :

- Connaître les enjeux techniques, méthodologiques et réglementaires liées à la protection des informations dans les réseaux et le rôle des techniques cryptographiques dans la mise en place des mécanismes de sécurité.
- Maîtriser les caractéristiques des algorithmes de chiffrement pour être en mesure de choisir le type d'algorithme en fonction des services de sécurité à mettre en place, selon des critères techniques et juridiques.
- Etendre ces connaissances à d'autres techniques de chiffrement et à leur mise en œuvre dans les entreprises.

Mots clefs :

-

Prérequis :

-

Programme:

- Sécurité de l'information dans les réseaux
 - Problématique et besoins de protection des réseaux
 - Cybercriminalité et infections informatiques
 - Architectures de sécurité Internet, Intranet et Extranet
 - Méthodologie d'analyse des risques (Méthodologie MEHARI)
 - Législation et Critères d'évaluation de la sécurité (ITSEC)
- Systèmes cryptographiques et leur mise en œuvre
 - Chiffrement symétrique ou à clé secrète (DES, IDEA)
 - Chiffrement asymétrique ou à clé publique (Diffie Hellman, RSA)
 - Chiffrement irréversibles (MDx, SHA, DSS)
 - Gestion et distribution des clés de chiffrement (PKI)
 - Confidentialité, Intégrité et Signature digitale
 - Applications : protocoles Kerberos, PGP
- Cryptographie et droit, à l'interception de l'ordre public et de la liberté
 - Statut actuel de la cryptographie : l'ordre public ; l'Arrangement de Wassenaar, les biens à double usage; la problématique de l'utilisation, de l'exportation, de l'importation aux USA et en Europe; le cas français
 - Cryptographie et interceptions de télécommunication
 - Cryptographie et commerce électronique : la problématique
 - Cryptographie et moyens de paiement : pistes et dysfonctionnement

Evaluation :

- 1^{ère} session = 1 contrôle écrit (C1)
- 2^{ème} session = 1 contrôle écrit (C2)
- Note finale = Sup (C1, C2)

Support de cours et bibliographie :

Polycopiés de cours

Bibliographie :

- Protection des systèmes d'information ,J.M. Lamere, P. Rose, J. Tourly , Les référentiels Dunod, 1999
- Sécurité dans les réseaux informatiques, D. W. Davies et W. L. Price, Seconde édition, AFNOR, 1995.
- Cryptographie appliquée, B. Schneier, International Thomson Publishing, 1995.
- Droit et sécurité des télécommunications, C. Guerrier, M.C. Monget, Springer France, Collection technique et scientifique des télécommunications, 2000
- Le COCOM et les exportations de produits informatiques, D. Puig ,mémoire de DEA, Montpellier, 1990

Responsable :

- Abdallah M'HAMED (Abdallah.Mhamed@it-sudparis.eu)

Intervenants :

- A. M'HAMED (TMPS)
- H. CHAOUCHI (TMPSP)
- C. GUERRIER (TMPSP)
- P. MAIGRON (TMSP)
- G. PELIKS (EADS)
- L. MOURER (BULL)