Licence : Systèmes Informatiques (SI)

Semestre (S5)

UF1 : Système d'exploitation 2

Objectifs de l'enseignement : Introduire la problématique du parallélisme dans les systèmes d'exploitation et étudier la mise en œuvre des mécanismes de synchronisation, de communication dans l'environnement centralisé

Connaissances requises : algorithmique, systèmes d'exploitation (L2)

Contenu de la matière

1. **Notions de parallélisme, de coopération et de compétition**
   - Systèmes de tâches, outils d'expressions
   - Déterminisme et parallélisme maximal
   - Threads
2. **Synchronisation**
   - Problème de l'exclusion mutuelle
   - Synchronisation
     - Evénements, Verrous
     - Sémaphores
     - Moniteurs
     - Régions critiques.
     - Expressions de chemins
3. **Communication**
   - Partage de variables (modèles : producteur/ consommateur, lecteurs/ rédacteurs)
   - Boites aux lettres
   - Echange de messages (modèle du client/ serveur)
   - Communication dans les langages évolués (CSP, ADA, JAVA..)
4. **Interblocage**
   - Modèles
   - Prévention
   - Evitement
   - Détection/ Guérison
   - Approche combinée
5. **Etude de cas : système Unix**
   - Principes de conception
   - Interfaces (programmeur, utilisateur)
   - Gestion de processus, de mémoire, des fichiers et des entrées/sorties
   - Synchronisation et Communication entre processus.

Références

- *J-L. Peterson, F. Silbershartz , P. B. Galvin '' Operating Systems Concepts,'' Fourth Edition.*
- *Crocus, '' Systèmes d'exploitation des ordinateurs,'' Dunod informatique 1975.*

UF1 : Compilation

Objectifs de l'enseignement : Introduction au problème de la compilation à savoir la traduction du texte-source au code assembleur ou autre. Il présente les différentes phases d'analyse et présente les outils de génération de compilateurs comme Lex et Yacc.

Connaissances requises : algorithmique, théorie des langages

Contenu de la matière

1. **Introduction à la Compilation**
    - Les différentes étapes de la Compilation
    - Compilation, Interprétation, Traduction
2. **Analyse lexicale**
    - Expressions régulières
    - Grammaires
    - Automates d'états finis
    - Un exemple de générateur d'analyseurs lexicaux : LEX
3. **Analyse syntaxique**
    - Définitions : grammaire syntaxique, récursivité gauche, factorisation d'une grammaire, grammaire ε-libre.
    - Calcul des ensembles des débuts et suivants.
    - Méthodes d'analyse descendantes : la descente récursive, LL(1).
    - Méthodes d'analyse ascendantes : LR(1), SLR(1), LALR(1), (méthode des items).
    - Un exemple de générateur d'analyseur syntaxique : YACC.
4. **Traduction dirigée par la syntaxe (Analyse sémantique)**
5. **Formes intermédiaires**
    - forme postfixée et quadruplés
    - triplés directs et indirects
    - arbre abstrait
6. **Allocation – Substitution- Organisation des données à l'exécution**
7. **Optimisation du code objet**
8. **Génération du code objet**

Références

- *Christopher Fraser and David Hanson. A Retargetable C Compiler : Design and Implementation. Benjamin/Cumming, 1995*
- *Compilateurs : principes, techniques et outils - A. Aho, R. Sethi, J. Ullman - InterEditions (disponible à la bibliothèque).*
- *Compilateurs - D. Grune, H. Bal, C. Jacobs, K. Langendoen - Dunod.*
- *Compîlation et Théorie des langages - S. Gire - Polycopié de cours IUP Informatique Brest.*

UF1 : Programmation logique

Objectifs de l'enseignement

- Initiation à la programmation en logique : application de certaines notions vues en cours de logique
- Découverte de la programmation en Prolog : utilisation d'exemples liés aux cours de théorie des langages et d'analyse et compilation.

Contenu de la matière :

- Programmation logique et Prolog
- Premiers pas en Prolog
- Bases du langage Prolog (structures de données simples)et Aspects avancés de Prolog (règles prédéfinies, entrées-sorties, mise au point des programmes)(Transparents PowerPoint du cours)
- Les listes
- Création et manipulation de listes
- Termes préfixés et N-Uplets
- Découverte de Gnu Prolog, Manipulation des N-Uplets et des arbres

Références

- *J. W. Lloyd, Fondements de la programmation en logique, Eyrolles, 1984.*
- *F. Giannesini, H. Kanoui, R. Pasero et M. Van Caneghem, Prolog, InterEditions, 1985.*

UF2 : Génie Logiciel 2

Contenu de la matière :

I- Processus de développement logiciel

1. Motivations
   1.1 Qualités attendues d'un logiciel
   1.2 Principes du Génie Logiciel
   1.3 Maturité du processus de développement logiciel

2. Cycle de vie d'un logiciel
   2.1 Composantes du cycle de vie d'un logiciel
   2.2 Documents courants
   2.3 Modèles de cycle de vie d'un logiciel
   2.4 Modèles de processus logiciels

II- Conduite de projets

3. Gestion de projets
   3.1 Pratiques critiques de la gestion de projet
   3.2 Analyse de la valeur acquise
   3.3 Suivi des erreurs

4. Planification de projets
   4.1 Organigramme technique
   4.2 La méthode PERT
   4.3 Autres modèles
   4.4 Estimation des coûts (Exp : Modèle COCOMO).

5. Assurance qualité

III- Techniques du Génie Logiciel

6. métriques
   6.1 Métriques de Mac Cabe
   6.2 Métriques de Halstead
   6.3 Métriques de Henry-Kafura
   6.4 Métriques Objet de Chidamber et Kemerer
   6.5 Métriques MOOD

7. Analyse et gestion des risques

8. Tests logiciels
   8.1 Tests fonctionnels
   8.2 Tests structurels
   8.3 Test de flot de données
   8.4 Tests orientes objet

Références

1. *Design Patterns: Elements of Reusable Object-Oriented Software. Erich Gamma, Richard Helm,Ralph Johnson, and John Vlissides. Addison Wesley. October 1994.*
2. *Objects, Components, and Frameworks with UML: The Catalysis(SM) Approach.Desmond D'Souza and Alan Wills. Addison-Wesley, 1998.*
3. *A UML Profile for Data Modeling. Scott Ambler*
4. *Multiple Inheritance in Java. Joseph Bergin*
5. *UML Resource Page: spécifications de l'OMG (UML, OCL, XMI): http://www.omg.org/uml*

UF2 : IHM

Objectifs de l'enseignement

L'objectif de ce cours est d'initier les étudiants à produire des logiciels ergonomiques tenant compte de l'aspect usager. Pour ce faire, il faut étudier les différents formalismes de spécification d'interfaces. Des exemples d'environnements sont également proposés. Il est recommandé d'effectuer des travaux pratiques sur un environnement d'interfaces homme-machine.

Contenu de la matière :

1- IHM, Interaction Homme-Machine : problématique et enjeux du domaine,
2- Apports de la Psycho Cognitive, Méthodes de conception
3- Principes d'Ergonomie des Logiciels, critères ergonomiques de qualité
4- Analyse des besoins, des acteurs et de leur activité, modélisation des activités
5- Principes de conception, spécification d'interfaces
6- Normes et de mesures pour les systèmes interactifs
7- Evaluation des interfaces
8- Toolkits Graphiques
   - Java : Swing
   - C++ : QT
   - Web :JQuery
9- IHM pour les interfaces mobiles.
10- Accessibilité

Références

- *David Benyon, Designing Interactive Systems: A Comprehensive Guide to HCI, UX and Interaction Design,Pearson; 3 edition, 2013*
- *Yvonne Rogers, Helen Sharp & Jenny Preece, Interaction Design: beyond human-computer interaction (3rd edition), Wiley, 2011*
- *Norman DA, The Design of Everyday Things, Basic Books, 2002. Serengul Smith-Atakan The FastTrack to Human-Computer Interaction, (Paperback)Thomson Learning, 2006.*
- *Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides, design Patterns, catalogue de modèles de conception réutilisables - International Thomson Publishing 1996*
- *Nathalie Lopez, Jorge Migueis, Emmanuel Pichon - Intégrer UML dans vos projets Eyrolles*
- *Bertrand Meyer - Conception et programmation orientées objet - Eyrolles*
- *Pascal Roques - UML-2, Modéliser une application WEB - Editions Eyrolles*
- *Kolski C.(editeur) "Environnements évolués et évaluation de l'IHM interaction Homme-Machine pour les systèmes d'ingormations, Volume 1 , Hermes, 2001*
- *B. Shneiderman "Designing the user Interface: Strategies for effective human computers" Edition Wesley, 1987.*
- *Coutaz J. "interface homme-ordinateur, conception et réalisation". Dunod informatique 1990*
- *Kolski C. (editeur) "Analyse et conception de l'IHM, interaction Homme-Machine pour les systèmes d'information", Volume &, Hermes, 2001.*
- *D. Floy et A. Vandam « Fundamentals of interactive computer graphics » Editon Wesley, 1983*

UM1 : Probabilités et statistiques

Objectifs de l'enseignement

Ce cours constitue une introduction à l'étude des modèles aléatoires simples. L'objectif est de fournir les outils indispensables dans le domaine des probabilités, et également d'aborder les aspects statistiques.
À la fin de ce module, l'étudiant devrait être en mesure de calculer les différentes mesures de dispersions dans les statistiques et d'effectuer des probabilités basées sur les lois de la probabilité et de faire des tests sur des données en utilisant les théories de la probabilité.

Contenu de la matière :

1. Espaces probabilisés
2. Variables aléatoires discrètes
3. Variables aléatoires continues
4. Fonctions caractéristiques
5. Théorèmes limites
6. Vecteurs gaussiens
7. Simulation
8. Estimateurs
9. Tests
10. Intervalle et régions de confiance
11. Problèmes (probabilités)
12. Problèmes (probabilités et statistique)

Références

- *Lecoutre B., Tassi Ph. (1987) Statistique non paramétrique et robustesse Paris : Economica.*
- *Tassi Ph. (1989) Méthodes statistiques Paris: Economica*
- *Tassi Ph., Legait S. (1990) Théorie des probabilités en vue des applications statistiques Paris : Ed. Technip*
- *Saporta, G., Probabilités, Analyse des données et Statistique, Technip, 2ème édition, 2006*
- *Jean-Pierre Lecoutre, Statistique et probabilités, Editions Dunod, 2012.*
- *Yadolah Dodge, Valentin Rousson, Analyse de régression appliquée, Editions Dunod, 2004.*

UM1 : Programmation linéaire

Objectifs de l'enseignement : Ce cours dresse un panorama des techniques de modélisation utilisées en programmation linéaire, il permet le développement d'applications industrielles en optimisation.

Connaissances requises : algèbre linéaire

Contenu de la matière :

1. **Rappels Mathématiques (Algèbre linéaire)**
    - Espace vectoriel
    - Dimension, base
    - Matrice, déterminant d'une matrice, inverse d'une matrice …
2. **Introduction et propriétés de la programmation linéaire**
    - Forme générale d'un programme linéaire, forme canonique, standard et mixte.
    - Résolution graphique, notion de polyèdre.
    - Résolution analytique.
3. **Méthode du simplexe**
    - Introduction de la méthode, algorithme du simplexe, tableau du simplexe
    - Méthodes particulières : méthode des pénalités, méthode des deux phases
    - Forme révisée du simplexe
4. **Dualité**
    - Introduction, règles de passage du primal au dual
    - Algorithme dual du simplexe
5. **Problème du transport**
    - Introduction du problème, graphe associé au tableau du transport
    - Algorithme du transport
    - Algorithme dual du transport.

Références

- *Christelle Gueret, Christian Prins, Marc Sevaux, Programmation linéaire, Edition Eyrolles, 2000.*
- *Pierre Borne, Abdelkader El Kamel, Khaled Mellouli, Programmation linéaire et applications, Editions Technip, 2004.*

UM1 : Paradigmes de programmation

Objectifs de l'enseignement

- se familiariser avec diverse paradigmes de programmation
- connaître les principes fondamentaux de divers paradigmes
- étudier les différences principales des paradigmes de programmation

Contenu de la matière :

1. Langages de programmation:
    a. vue générale
    b. historique (assembleur, langage évolué)

2. Paradigmes: introduction
3. Programmation impérative
4. Programmation fonctionnelle
5. Programmation orientée objet
6. Programmation orientée aspect
7. Paradigmes composant, agent et service
8. Programmation logique

Références

- *Essentials of Programming Languages, 2nd Edition, D.P. Friedman, M. Wand, C.T. Haynes. MIT Press, 2001, http://www.cs.indiana.edu/eopl/*
- *Structure and Interpretation of Computer Programs, H. Abelson, G.J. Sussman, J. Sussman. MIT Press, 198, http://mitpress.mit.edu/sicp/full-text/book/book.html*
- *How to Design Programs: An Introduction to Programming and Computing, Matthias Felleisen, Robert Bruce Findler, Matthew Flatt, Shriram Krishnamurthi. MIT Press, 2002, http://www.htdp.org*
- *The Schematics of Computation, Vincent Manis, James Little. Prentice Hall, 1995, http://cs.ubc.ca/spider/little/schematics.html*

UM1 : Intelligence artificielle

Objectifs de l'enseignement : inculquer à l'étudiant des notions de base en intelligence artificielle comme la nature de l'IA, la représentation des connaissances, la résolution des problèmes, etc. La programmation logique et les systèmes experts sont également abordés pour attribuer un caractère pratique à cet enseignement.

Connaissances requises : Logique mathématique

Contenu de la matière

1. **Introduction**
   a. Histoire de l'IA
   b. Nature de l'IA
2. **Représentation des connaissances**
   a. Notion de connaissance et extraction de connaissances
   b. Représentations logiques
   c. Représentation à base de règle de production
3. **Systèmes experts**
   a. Définition et architecture d'un système expert
   b. Raisonnement à base de règles de production
   - Chainage avant
   - Chainage arrière
4. **La programmation logique**
   c. Le langage Prolog
   d. Syntaxe et structures de données – opérateur de coupure
   e. Le problème de la négation en PROLOG : l'hypothèse du monde clos et la négation par échec.
   f. Utilisation de la méthode de résolution dans l 'implantation machine de ce type de langage.

Références

1. *Louis Gacôgnes, Prolog : Programmation par l'exemple, 2009.*
2. *Manuel d'intelligence artificielle, L. Frécon, O. Kazar, édition PPUR, 2009*
3. *N.J. Nilsson, principes d'intelligence artificielle, Cepadues-Editions, 1988.*
4. *Louis Gacôgnes, Prolog : Programmation par l'exemple, 2009.*

UT1 : Anglais

Objectifs de l’enseignement

Compréhension, connaissance et utilisation active des notions linguistiques fondamentales à l'écrit et à l'oral, dans le cadre de situations de la vie quotidienne et professionnelle.

Acquisition de connaissances lexicales et méthodologiques en anglais scientifique et technique permettant la compréhension globale de documentations du secteur informatique en particulier.

Contenu de la matière :

Ce module devrait être enseigné à travers des documents issus du domaine et de l’actualité (Journaux, documentaires audio, vidéo, ...etc.).

Références bibliographiques

- *Documents d’actualité.*
- *Articles scientifiques*

Licence : Systèmes Informatiques (SI)

Semestre (S6)

UF3 : Développement d'applications mobiles

Objectifs de l'enseignement : présenter les systèmes d'exploitations mobiles ainsi que les plateformes de développement des applications mobiles. L'étudiant aura l'occasion de découvrir le développement d'applications dédiées aux réseaux sans fil.

Connaissances requises : algorithmique, connaissance sur le web, POO

Contenu de la matière :

1. **Introduction**
2. **Architecture et fonctionnalités de base de la plate-forme Android**
3. **Préparation et installation de l'environnement de développement**
    - **Emulation d'un appareil mobile**
4. **Les systèmes d'exploitation mobiles**
    - iOS
    - Android
    - WindowsPhone
5. **Structure et composants fondamentaux des applications mobiles**
6. **Construction de l'interface utilisateur ;**
7. **Utilisation des ressources : XML, images, fichiers, etc.**
8. **Programmation mobile avec Android**
    - Le SDK Android
    - XML et JSON
    - Eléments d'interface
    - Les bases de données avec SQLite
    - Connectivité
9. **Développement d'une application simple (étape d'intégration)**
10. **Déploiement d'une application mobile.**

Références

- *Nazim BENBOURAHLA, Android 4, Les fondamentaux du développement d'applications Java, Editions ENI, 2012.*
- *Mark Murphy, L'art du développement Android, Pearson Education, 2009.*
- *André, F., & Segarra, M. T. (2000). MolèNE: un système générique pour la construction d'applications mobiles. Numéro spécial" Evolution des plates-formes orientées objets répartis, 12.*
- *David, R. (2003). Architecture reconfigurable dynamiquement pour applications mobiles (Doctoral dissertation, Rennes 1) (résumé).*
- *Garin, F. (2009). ANDROID: Développer des applications mobiles pour les Google Phones. Dunod.*
- *Garin, F. (2011). Android-Concevoir et développer des applications mobiles et tactiles-2ème édition.: Concevoir et développer des applications mobiles et tactiles. Dunod.*
- *Gonzalez, C., Huré, E., & Picot-Coupey, K. (2012, November). http://thil-memoirevivante.prd.fr/sites/thil-memoirevivante.prd.fr/IMG/pdf/Gonzalez_Hure_Picot-Coupey.pdf Usages et valeurs des applications mobiles pour les consommateurs: quelles implications pour les distributeurs?]. In 15ème colloque Etienne Thil.*
- *Kaddour, M. (2004). etPautet L.,«Une approche coopérative des applications mobiles basées sur MobileJMS». Premières journées francophones sur Mobilité et Ubiquité, Nice, France.*
- *Google Android training here https://developer.android.com/training/index.html*
  J.F. DiMarzio, Android A Programmer's Guide, 2008 McGraw-Hill

UF3 : Sécurité informatique

Objectifs de l'enseignement

Présenter aux étudiants les problèmes de sécurité posés par les ressources informatiques et réseaux et leur décrire les outils cryptologiques qui répondent à ces problèmes.

Contenu de la matière :

1- Principes de la sécurité

1.1 Exigences Fondamentales
1.2 Étude des risques
1.3 Établissement d'une politique de sécurité
1.4 Eléments d'une politique de sécurité
1.5 Principaux défauts de sécurité
1.6 Eléments de droits

2- Failles de sécurité sur internet

2.1 Définitions
2.1.1 IP spoofing
2.1.2 DNS spoofing
2.1.3 Flooding
2.1.4 Smurf
2.1.5 Web bug
2.1.6 Hoax (rumeur)
2.1.7 Hacker et cracker

2.2 Principales attaques
2.2.1 Virus
2.2.2 Déni de service (DoS)
2.2.3 Écoute du réseau (sniffer)
2.2.4 Intrusion
2.2.5 Cheval de Troie
2.2.6 Social engineering

3- Protections

3.1 Formation des utilisateurs

3.2 Poste de travail

3.3 Antivirus

3.4 Pare-Feu (FIRE WALL)

3.4.1 Architecture classique
3.4.2 Architecture concentrée
3.4.3 Logiciels
3.4.4 Filtrage de sites

3.5 Authentification et cryptage

3.5.1 Cryptage symétrique
3.5.2 Cryptage asymétrique
3.5.3 Protocoles courants
3.5.4 PKI (Public Key Infrastructure)

3.6 Messageries

3.6.1 Attaques
3.6.2 Sécurité des messages
3.6.3 Spamming

3.7 Détection d'intrusion

3.7.1 Surveillance du trafic réseau
3.7.2 Analyse du comportement de l'utilisateur
3.7.3 Site « pot de miel »

3.8 Où AGIR

3.9 Tests

3.9.1 Tests de maintenance
3.9.2 Logiciels de test de la sécurité d'une installation
3.9.3 Certification des produits de sécurité

Références

- *Cours de cryptographie, Gilles Zémor, Cassini, 2000.*
- *Cryptography, Theory and Practice, 3ème édition, Douglas Stinson, Chapman and Hall, 2002.*
- *Introduction to cryptography with coding theory, 2ème édition, Wade Trappe and Lawrence C. Washington, 2ème édition, 2006.*
- *An Introduction to Coding Theory, 3ème édition, van Lint, Springer, 1998.*
- *The theory of error-correcting codes, 11ème édition, MacWilliams and Sloane, North-Holland, 2003.*
- *Information and Coding Theory, G. A. Jones and J. M. Jones, Springer, 2000.*

UF4 : Administration de BD

Objectifs de l'enseignement

Cet enseignement donne des bases théoriques et pratiques sur des notions concernées directement dans la conception et l'administration des bases de données : dictionnaire de données, bases de données transactionnelles et accès concurrents, sécurité des données (reprise après panne) et sécurité des accès, optimisation des requêtes et gestion des performances (tuning) des bases de données.

Contenu de la matière

1. Rappel : Conception et optimisation de schéma relationnel :
   notion de redondance, dépendance fonctionnelle, formes normales.
2. Administration des BDs : dictionnaire de données, import/export (SQL Loader)
3. Objects avancés : vues, index, déclencheurs
4. Politiques de contrôle des accès
5. Transactions et sécurité des données :
   résistance auxpannes, accès concurrents,interblocages, verrouillage , estampillage
6. Optimisation : indexation et optimisation de requêtes
7. Informations incomplètes dans les bases de données
8. Bases de données semi-structurées et XML
9. Interrogation (Xquery, Xpath, ...)
10. Bases de données multimédias (modélisation, interrogation)

Travaux Dirigés

1. PL/SQL
2. Indexation et accès concurrents (schémas sérialisables)
3. Indexation et optimisation de requêtes

Travaux Pratiques

- PL/SQL
- Administration Oracle

1. Installation de la base (fichiers de configuration de la base)
2. Gestion des sessions (montage et démontage d'instance de base)
3. sécurité des données : gestion des utilisateurs, vues, fonctions d'audit
4. Intégrité des données : programmation descontraintes d'intégrité et des triggers
5. Sauvegarde et Restauration de la base, modes d'archivage de la base
6. Gestion de la performance (tuning)

Références

- *Date C.J. (2000) Introduction aux bases de données (7° édition), Vuibert.*
- *Chrisment C. (2008) Bases de données relationnelles : concepts, mise en œuvre et exercices, Hermès*
- *Gardarin.G (1990). SGBD avancés, Eyrolles*
- *Gardarin.G. (1999) Bases de données : objet et relationnel, Eyrolles.*
- *Gray J., Andreas R. (1993) Transaction processing: concept and techniques. Morgan Kaufman*
- *Soutou.C] (2008). SQL pour Oracle avec 50 exercices corrigés,(3ème édition) ; Eyrolles*
- *Briard G. (2006) Oracle 10g sous Windows, Eyrolles, Paris.*

UF4 : Infographie

Objectifs de l'enseignement

L'**infographie** est le domaine de la création et la manipulation d'images numériques par des moyens informatique. Cette matière ayant pour objectif d'introduire le domaine de l'infographie aux étudiants et de les rendre aptes à manipuler les outils graphiques et à traiter et exploiter des éléments du multimédia tels les images et les animations 2D/3D et la vidéo.

Contenu de la matière :

Chapitre 01 : Introduction

- Notions fondamentales de l'infographie
- Domaines de l'infographie (traitement d'image, synthèse d'images, reconnaissance des formes….)
- Outils et API graphiques
- Applications

Chapitre 02 : Bases géométriques pour l'infographie

- Géométrie analytique dans le plan
- Géométrie analytique dans l'espace
- Primitives graphiques

Chapitre 03 : L'image et la vidéo

- Principe de formation d'une image
- Structure d'une image numérique
- Image aux niveaux de gris et image couleur
- Image matricielle et image vectorielle
- Les formats d'image et ses caractéristiques
- La vidéo
- Caractéristiques des formats vidéo

Chapitre 04 : Traitement d'images

- Principe
- Traitements de base
- Applications

Chapitre 05 : Synthèse d'images

- Principe
- Modélisation
- Rendu
- Animation
- Applications

Références

1. ***Introduction a l'infographie*** *- Steven k. FEINER, James d. FOLEY, John f. HUGHES, Richard l. PHILLIPS, Andries VAN DAM , VUIBERT EDITION ,2000 ;*
2. ***La boîte à outils du graphiste débutant - 20 projets créatifs à réaliser pas à pas*** *- Tony Seddon , Jane Waterhouse , Edition Dunod – Juin 2010.*
3. ***Géométrie analytique,*** *Laurent Vivier, Editions Le Pompier, 2006*
4. ***Initiation à la synthèse d'images,*** *Pascal Mignot, Cours de Maîtrise d'informatique, Université de Reims- France ;*
5. ***http://raphaello.univ-fcomte.fr/ig/Default.htm***
6. ***http://www.cgeo.ulg.ac.be/infographie/***

UF4 : Web sémantique

Objectifs de l'enseignement

Ce cours est une présentation approfondie des techniques de représentation de connaissance mises en œuvre dans le cadre du Web sémantique. Son but est de présenter, dans ce cadre précis, les résultats obtenus sur la sémantique des représentations de connaissance, les problèmes posés par leur mise sur le réseau ainsi que les problèmes de recherche que cela pose.

Contenu de la matière :

- Introduction au web sémantique
    1. Le web sémantique
    2. Ressources disponibles
    3. Modéliser le domaine d'application
    4. Exprimer les données
    5. Manipuler les données
- Théorie des modèles
    1. Une vision abstraite de la logique
    2. La logique des propositions
    3. La logique des prédicats
- Graphes conceptuels
    1. Exemple
    2. Syntaxe
    3. Projection et morphisme
    4. Sémantique donnée par traduction
    5. Complexité et conclusion
- RDF
    1. RDF Simple : syntaxe
    2. RDF Simple : sémantique
    3. RDF : syntaxe
    4. RDF : sémantique
- RDF Schéma
    1. Sémantique
    2. Projection et conséquence sémantique
    3. Correction et complétude
- Logiques de description et OWL
    1. AL : Syntaxe
    2. Sémantique
    3. Mécanisme de résolution (tableaux sémantiques)
    4. Expressivité et complexité
    5. Une introduction à OWL

Références

- *T. Berners-Lee, J, Hendler, Ora Lassila, The Semantic Web, Scientific American, 2001.*
- *Jérôme Euzenat, Pavel Shvaiko, Ontology matching, Springer-Verlag, Heidelberg (DE), 2007.*

UF4 : Cryptographie

Objectifs de l'enseignement

L'étudiant, après avoir suivi ce cours, doit être capable de :
- utiliser le système de clé publique et privée pour chiffrer et déchiffrer les messages.
- utiliser les certificats d'authentification.
- chiffrer et déchiffrer les messages à l'aide des techniques anciennes et modernes de cryptographie.

Contenu de la matière :

1. Notions de base : terminologie, fonctions cryptographiques ; exemples historiques de protocoles de cryptographie : la scytale, le cryptogramme de César, la permutation de lettres, le chiffrement de Vigenère, le chiffrement de Hill ; protocoles de confidentialité : protocoles à clé secrète et à clé publique, quelques principes de base ; cryptanalyse.
2. Fonctions booléennes : définition ; fonctions booléennes et opérateurs logiques ; fonctions booléennes et polynômes de F2[X1,...,Xn] ; conversion entre représentations normales ; distance ; transformées de Fourier et de Walsh ; fonctions booléennes vectorielles.
3. Cryptographie à clé secrète : propriétés ; nombres binaires et hexadécimaux ; codage par blocs : ECB et CBC ; diagrammes de Feistel ; D.E.S. (Data Encryption Standard) ; I.D.E.A. (International Data Encryption Algorithm).
4. Le protocole A.E.S. : présentation ; les quatre étapes d'une ronde ; Extensions de F2 et le corps A.E.S. ; L'étape SubBytes ; L'étape ShiftRows ; L'étape MixColumns ; L'étape AddRoundKey ; Expansion de la clé; résultats de cryptanalyse contre A.E.S.
5. Cryptanalyse des protocoles à clé secrète : confusion et diffusion ; cryptanalyse linéaire : fonctions linéaires, résistance linéaire, biais, approximation linéaire, attaque par cryptanalyse linéaire.
6. Cryptographie à clef publique (RSA, logarithme discret)
7. Fonctions de hachage et signature électronique
8. Architectures PKI, SSL

Références

- *David Kahn (trad. Pierre Baud, Joseph Jedrusek), La guerre des codes secrets [« The Codebreakers »], InterEditions, 1980, 405 p. (ISBN 2-7296-0066-3).*
- *Simon Singh (trad. Catherine Coqueret), Histoire des codes secrets [« The Code Book »], Librairie Générale Française (LFG), coll. « Le Livre de Poche », 3 septembre 2001, Poche, 504 p. (ISBN 2-253-15097-5, ISSN 0248-3653, OCLC 47927316).*
- *Jacques Stern, La science du secret, Odile Jacob, coll. « Sciences », 5 janvier 1998, 203 p. (ISBN 2-7381-0533-5, OCLC 38587884)*
- *Non mathématique.*
- *"Handbook of Applied Cryptography", http://cacr.uwaterloo.ca/hac/*
- *Schneier B. "Cryptographie Appliquée", https://www.schneier.com/book-applied.html*

UT2 : Rédaction scientifique

Objectifs de l'enseignement : Ce cours apprend à l'étudiant la méthodologie pour élaborer un travail scientifique. Il l'assiste dans les opérations de rédaction et de présentation de ses contributions.

Connaissances requises : rien

Contenu de la matière :

1. Démarche scientifique pour aborder les problématiques
2. Recherche et collecte de la documentation
3. Démarche de rédaction: compte-rendu, rapport, mémoire de fin d'étude, article de recherche
4. Templates
5. Démarche de présentation d'un travail d'étude ou de recherche
6. Les règlements universitaires
7. La fraude et le plagiat

Références :

- *L. Blaxter, C. Hughes & M. Tight, How to Research Buckingham: Open University Press, 1998.*
- *J. Collis, R. Hussey, Business Research: a practical guide for undergraduate and postgraduate students,Second edition, Basingstoke: Palgrave Macmillan, 2003.*
- *M, Denscombe, Ground Rules for Good Research, Maidenhead: Open University Press, 2002.*
- *M, Saunders, P. Lewis, A. Thornhil,Research Methods for Business Students, 4th edition, Harlow, Prentice Hall, 2006.*
- *M-L. Gavard-Perret, D. Gotteland, C. Haon, A. Jolibert, Méthodologie de la Recherche - Réussir son mémoire ou sa thèse en sciences gestion Pearson Education Universitaire B&E, 2008.*