REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

HARMONISATION

OFFRE DE FORMATION MASTER

ACADEMIQUE

Etablissement	Faculté / Institut	Département
Université Batna 2	**Faculté de mathématiques et de l'informatique**	**Informatique**

Domaine : Mathématiques - Informatique

Filière : Informatique

Spécialité : Cryptographie et Sécurité

Année universitaire : 2016-2017

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مواءمة

عرض تكوين ماستر

أكاديمي / مهني

المؤسسة	الكلية/ المعهد	القسم
جامعة باتنة 2	**رياضيات و الأعلام الآلي**	قسم الإعلام الآلي

الميدان : **رياضيات و الأعلام الآلي**

الشعبة : الإعلام الآلي

التخصص : تشفير و أمن

السنة الجامعية: **2016-2017**

SOMMAIRE

I – Fiche d’identité du Master
(Tous les champs doivent être obligatoirement remplis)

1 - Localisation de la formation :

Faculté : Mathématiques et de l'informatique
Département : Informatique

2- Partenaires de la formation *:

- autres établissements universitaires :

- entreprises et autres partenaires socio économiques :

- Partenaires internationaux :

* = Présenter les conventions en annexe de la formation

3 – Contexte et objectifs de la formation

A – Conditions d'accès *(indiquer les spécialités de licence qui peuvent donner accès au Master)*

Après étude du dossier par l'équipe de formation, ce master est accessible aux étudiants ayant :

- *Une licence académique d'informatique LMD,*
- *Une licence académique de Mathématiques LMD.*

B - Objectifs de la formation *(compétences visées, connaissances pédagogiques acquises à l'issue de la formation- maximum 20 lignes)*

L'objectif du master proposé et de former des cadres à profil d'experts spécialisés dans les domaines de la cryptologie et de la sécurité informatique. Ses diplômés auront une solide formation théorique en mathématiques et en informatique, compétences qu'ils verront appliquées à des problèmes pratiques en cryptographie et sécurité dans les entreprises privées et publiques.

Plus précisément, ce master permettra aux étudiants de :

1) Acquérir les notions fondamentales :
   - En mathématiques (algèbre, arithmétique),
   - En informatique (algorithmique, théorie de la complexité, programmation orientée objet),

2) Maîtriser les outils spécifiques au traitement de l'information (codes correcteurs d'erreurs, cryptographie, algorithmique arithmétique, traitement de signal et de l'image, sécurité des réseaux, etc.).

3) Explorer et maitre en œuvre les notions étudiées en vue de développer des cryptosystèmes pour la protection de l'information.

C – Profils et compétences métiers visés *(en matière d'insertion professionnelle - maximum 20 lignes) :*

La spécialité proposée vise à former des doctorants en informatique.

Les applications visées sont

Traitement et protection de l'information, tels que :

- Sécurité des réseaux (toutes entreprises)
- Sécurisation des transactions sur Internet (banques, services…)
- Télécommunications
- Cryptographie (carte à puces, secteur militaire).

D- Potentialités régionales et nationales d'employabilité des diplômés

Dans tous les domaines : entreprises, enseignement, administrations, recherche.

E – Passerelles vers d'autres spécialités

Certaines spécialités en Informatique et en Mathématiques appliquées.

F – Indicateurs de suivi de la formation

Le suivi des enseignements se fera par le comité pédagogique de la formation composé des coordonnateurs de la formation, des enseignants intervenants et des délégués des étudiants (si nécessaires).

Ce comité se réunira trois fois par semestre au minimum et aura pour tâches

- de mettre au point des méthodes pédagogiques adéquates avec les objectifs visés,
- d'évaluer les enseignements et la formation (état d'avancement et autres),
- de mettre en place le parrainage des étudiants,
- de veiller à la cohérence du parcours et des stages,
- de faire le suivi des séminaires et des mémoires,
- d'évaluer le travail des étudiants.

Les PV des réunions seront transmis régulièrement aux :

- Chef de département d'informatique.
- Président du comité scientifique du département,
- Chefs des laboratoires impliqués,

Vice doyen chargé de la pédagogie de la faculté des sciences de l'ingénieur.

G – Capacité d'encadrement (donner le nombre d'étudiants qu'il est possible de prendre en charge)

30 postes

(Précisément 20 étudiants informaticiens et 10 étudiants mathématiciens)

4– Moyens humains disponibles

A : Enseignants de l'établissement intervenant dans la spécialité :

Nom, prénom	Diplôme graduation + Spécialité	Diplôme Post graduation + Spécialité	Grade	Type d'intervention *	Emargement
Noui Lemnouar		**Doctorat, Algèbre**	**Professeur**	**Cours, TD, TP, Encadrement de mémoires**	
Melekmi Lamine		**Doctorat, Mathématiques**	**Professeur**	**Cours, TD, TP, Encadrement de mémoires**	
Abdessemed Fodil		**Doctorat, Electronique**	**Professeur**	**Cours, TD, TP, Encadrement de mémoires**	
Seghir Rachid		**Doctorat, Informatique**	**M.C. classe A**	**Cours, TD, TP, Encadrement de mémoires**	
Behloul Ali		**Doctorat, Informatique**	**M.C. classe B**	**Cours, TD, TP, Encadrement de mémoires**	
Hamouid Khaled		**Magister, Informatique**	**M.A. classe A**	**Cours, TD, TP, Encadrement de mémoires**	
Guitoune Abdelhafid		**Ingéniorat, Informatique**	**Assistant**	**Cours, TD, TP, Encadrement de mémoires**	
Toumi Mohamed		**Magister, Informatique**	**M.A. classe A**	**Cours, TD, TP, Encadrement de mémoires**	

Betta Mohamed		**Magister, Informatique**	**M.A. classe A**	**Cours, TD, TP, Encadrement de mémoires**	
Dekhinet Abdalhamid		**Magister, Informatique**	**M.A. classe A**	**Cours, TD, TP, Encadrement de mémoires**	
Benzeghli Brahim		**Doctorat, Mathématiques**	**M.C. classe B**	**Cours, TD, TP, Encadrement de mémoires**	
Djellab Rima		**Magister, Informatique**	**M.A. classe A**	**Cours, TD, TP, Encadrement de mémoires**	

*** = Cours, TD, TP, Encadrement de stage, Encadrement de mémoire, autre (à préciser)**

B : Encadrement Externe :

Etablissement de rattachement :

Nom, prénom	Diplôme graduation + Spécialité	Diplôme Post graduation + Spécialité	Grade	Type d'intervention *	Emargement

*** = Cours, TD, TP, Encadrement de stage, Encadrement de mémoire, autre (à préciser)**

5 – Moyens matériels spécifiques disponibles.

A- Laboratoires Pédagogiques et Equipements : Fiche des équipements pédagogiques existants pour les TP de la formation envisagée (1 fiche par laboratoire)

Intitulé du laboratoire : Laboratoire des applications des mathématiques à l'informatique et à l'électronique (LAMIE).

Capacité en étudiants : 30

N°	Intitulé de l'équipement	Nombre	Observations
01	Data Général machine Bi processeur 30 postes – Opérant sous Unix	01	
02	Centre de calcul équipe de 15 PC	03	
03	Imprimante réseaux	01	
04	Cluster de 8 PC – connexion à EumedGrid en projet	01	
05	Point d'accès internet Wireless	02	
06	Serveur Dell Bi-Processeurs	02	
07	Bibliothèque spécialisée –200 Ouvrages	01	
08	Amphithéâtres	03	
09	Salle de conférences pour séminaires	01	
10	Salles de TD	29	

B- Terrains de stage et formation en entreprise :

Lieu du stage	Nombre d'étudiants	Durée du stage

C- Laboratoire(s) de recherche de soutien au master :

Chef du laboratoire
N° Agrément du laboratoire
Date : Avis du chef de laboratoire:

D- Projet(s) de recherche de soutien au master :

Intitulé du projet de recherche	Code du projet	Date du début du projet	Date de fin du projet

E- Espaces de travaux personnels et TIC :

- Bibliothèque de la Faculté de mathématiques et de l'informatique,
- Bibliothèque des Laboratoires de recherche,
- Bibliothèque Centrale de l'Université,
- Connexion Internet.

II – Fiche d’organisation semestrielle des enseignements

(Prière de présenter les fiches des 4 semestres)

1- Semestre 1 :

Unité d'Enseignement	VHS	V.H hebdomadaire				Coeff	Crédits	Mode d'évaluation	
	14-16 sem	C	TD	TP	Autres			Continu	Examen
UE fondamentales						**9**	**18**	40%	60%
UEF1(O/P)									
M1 : Eléments d'algèbre pour la cryptographie	67h30	1h30	3h		82h30	3	6	x	x
UEF2(O/P)									
M1 : Eléments de combinatoire	67h30	1h30	1h30	1h30	82h30	3	6	x	x
M2 : Traitement de signal	67h30	1h30	1h30	1h30	82h30	3	6	x	x
UE méthodologie						**5**	**9**		
UEM1(O/P)									
Programmation orientée objet 1	60h	1h		3h	65h00	3	5	x	x
UEM2(O/P)									
Introduction à la cryptographie	45h	1h30		1h30	55h	2	4	x	x
UE découverte						**2**	**2**		
UED1(O/P)									
:Anglais 1	45h	3h			5h	2	2	x	x
UE transversales						**1**	**1**		
UET1(O/P)									
Protection des systèmes d'exploitation	22h30	1h30			2h30	1	1	x	x
Total Semestre 1	**375**	172h30	90h	112h30	**375**	**17**	**30**		

2- Semestre 2 :

Unité d'Enseignement	VHS	V.H hebdomadaire				Coeff	Crédits	Mode d'évaluation	
	14-16 sem	C	TD	TP	Autres			Continu	Examen
UE fondamentales						**9**	**18**		
UEF1(O/P)								40%	60%
M1 : Théorie des codes linéaires	67h30	1h30	3h		82h30	3	6	x	x
Matière2 : Réseaux	67h30	1h30	1h30	1h30	82h30	3	6	x	x
UEF2(O/P)									
Matière 1 : Complexité algorithmique et chiffrement	67h30	1h30	1h30	1h30	82h30	3	6	x	x
UE méthodologie						**5**	**9**		
UEM1(O/P)									
Matière 1 : Programmation orientée objet 2	60h00	1h		3h	65h00	3	5	x	X
Matière2 : Calcul formel	45h	1h30		1h30	55h	2	4	x	x
UE découverte						**2**	**2**		
UED1(O/P)									
Chiffrement audio	45h	1h30		1h30	5h	2	2	x	x
UE transversales						**1**	**1**		
UET1(O/P)									
Anglais 2	22h30	1h30			2h30	1	1	x	x
Total Semestre 2	**375**	150h	90h	135h	**375**	**17**	**30**		

3- Semestre 3 :

Unité d'Enseignement	VHS	V.H hebdomadaire				Coeff	Crédits	Mode d'évaluation	
	14-16 sem	C	TD	TP	Autres			Continu	Examen
UE fondamentales						**9**	**18**	40%	60%
UEF1(O/P)									
Matière 1 : Cryptographie avancée	67h30	1h30	1h30	1h30	82h30	3	6	x	x
Matière2 : Sécurité informatique	90h00	3h		3h	110h	4	7	x	x
Matiere 3 : Image et sécurité	45h00	1h30		1h30	55h	2	5	x	x
UE méthodologie						**5**	**9**		
UEM1(O/P)									
M1 : EDI et commerce électronique	60h	1h		3h	65h00	3	5	x	x
M2: Sûreté de fonctionnement des systèmes informatiques	45h	1h30	1h30		55h00	2	4	x	x
UE découverte						**2**	**2**		
UED1(O/P)									
Matière 1 : Méthodologie de recherche	45h	1h30	1h30		5h	2	2	x	x
UE transversales						**1**	**1**		
UET1(O/P)									
Matière 1 : Ethique et déontologie	22h30	1h30			2h30	1	1	x	x
Total Semestre 3	**375**	195h	67h30	135h	**375**	**17**	**30**		

4- Semestre 4 :

Domaine : Mathématiques-Informatique
Filière : Informatique
Spécialité : Cryptographie et Sécurité

Stage en entreprise sanctionné par un mémoire et une soutenance.

	VHS	Coeff	Crédits
Travail Personnel	375h	17	30
Stage en entreprise			
Séminaires			
Autre (préciser)			
Total Semestre 4	375h	17	30

5- Récapitulatif global de la formation : (indiquer le VH global séparé en cours, TD, pour les 04 semestres d'enseignement, pour les différents types d'UE)

UE / VH	UEF	UEM	UED	UET	Total
Cours	225	112.5	135	67.5	540
TD	202.5	0	22.5	0	225
TP	180	180	0	0	360
Travail personnel	742.5	360	225	112.5	1440
Autre (préciser)					
Total	1350	652.5	382.5	180	2565
Crédits	72	36	8	4	**120**
% en crédits pour chaque UE	60%	30%	6,6%	3.3%	100%

III - Programme détaillé par matière

(1 fiche détaillée par matière)

Intitulé du Master : Cryptographie et Sécurité

Semestre : 1

UEF1

Intitulé de la matière : Eléments d'algèbre pour la cryptographie.

Crédits : 6

Coefficients : 3

Objectifs de l'enseignement

La première partie introduit les notions fondamentales pour la théorie des groupes, des notions utiles pour la compréhension des corps et les codes linéaires ainsi que leurs applications. la deuxième partie devrait permettre à l'étudiant d'acquérir les connaissances élémentaires que procure la théorie des corps finis.

Connaissances préalables recommandées

Algèbre 1 et Algèbre 2

Contenu de la matière :

Partie 1

1. Groupes, exemples
2. Homomorphismes
3. Sous groupes, sous groupes distingués et groupes quotients.
4. Groupes cycliques, ordre des éléments, indice d'un sous groupe.
5. centre, centralisateur, conjugaison,.
6. groupes particuliers.
7. Groupes de permutations, groupes de matrices
8. Exemples d'application en cryptographie

Partie 2

1. Définitions, caractéristiques, cardinal d'un corps fini,
2. Relation de frobenuis, morphisme de Frobenuis,
3. Construction et unicité des corps finis, construction pratique de Fq,
4. Sous corps d'un corps fini. élément primitif, polynôme primitif.
5. polynômes irréductibles et éléments conjugués.
6. Factorisation de x^n -1,
7. Congruences et Classes résiduelles.
8. Fonction Phi d'Euler, les Théorèmes de Fermat, Euler et de Lagrange.
10. Les résidus quadratiques.
11. Suites récurrentes et registre à décalage.
12. Exemples d'applications : clés cryptographiques

Mode d'évaluation : Continu et examen.

Références

1. J. Querre, Cours d'algèbre, Maitrise de Mathématiques, Masson. 1976.
2. J. Calais. Éléments de théorie des groupes. PUF, 1998.
3. E. Ramis, C. Deschamps, et J. Odoux. Cours de Mathématiques 1, Algèbre. Dunod, 1998.
4 D.J.S. Robinson, "A course in the Theory of Groups," 2nd ed., Springer-Verlag, New York, 1995.
5. Rudolf Lid land Harald Niederreiter, Finite fields, Encyclopedia of Mathematics and applications, Cambridge university press, 1997.
6. M. Demazure. Cours d'algèbre. Primalité, divisibilité, codes. Cassini, 1997.

Intitulé du Master : Cryptographie et Sécurité

Semestre : 1
UEF2
Intitulé de la matière : Eléments de combinatoire
Crédits : 6
Coefficients : 3

Objectifs de l'enseignement

Les fondements mathématiques de la modélisation et le traitement de l'information numérique font intervenir plusieurs branches des mathématiques comme l'Algèbre, la Combinatoire et la théorie des graphes.

Connaissances préalables recommandées

Algèbre 1 et Algèbre 2

Partie I : Combinatoire énumérative

1. Application d'un ensemble E dans un ensemble Φ.
2. Applications particulières (injectives, surjectives, bijectives).
3. Relations binaires.
4. . Notion de cardinal. Ensembles finis. Ensembles dénombrables.
5. dénombrement des ensembles.

Partie II : Théorie des graphes pour la cryptographie.

1. Graphes simples
2. Matrice associée au graphe.
3. Arbre
4. Coloration d'un graphe.
5. Graphes particuliers (graphes hamiltoniens, graphes orientés,…)
6. Problèmes complexes liés aux graphes.
7. Graphes et cryptographie.

Références.

1. Francette BORIES « Graphes et combinatoire », Université Pierre et Marie Curie LM 226 (2010-2011).
2. Antoine Gournay, 'Théorie des graphes' Institut de Mathématiques, Université de Neuchâtel Suisse, Septembre, 2013.
3. Brice Halimi, « Structures et généralité en théorie combinatoire : les mathématiques et les lettres » Université Paris Ouest,, IREPH & SPHERE.
4. [Cameron, 1994] Cameron P. (1994), *Combinatorics: Topics, Techniques, Algorithms*, Cambridge UP, Cambridge.

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 1

UEF2

Intitulé de la matière : Traitement de signal

Crédits : 6

Coefficients : 3

Objectifs de l'enseignement

Cette UE permet aux étudiants d'acquérir les connaissances et les outils du traitement du signal, Ces notions sont utilisées pour accélérer certains algorithmes, en particulier les transformations de Fourrier sont indispensables pour le décodage de certains codes.

Connaissances préalables recommandées

Outils mathématiques de la première année,

Contenu de la matière

1. **Généralités sur les signaux,**
   Signal- définition
   Notation des signaux
   Classification des signaux
   Caractérisation des signaux (énergie, puissance d'un signal…)
   Exemples de quelques signaux particuliers (Dirac, Echelon, sinc,,,,,)
2. **Théorie de l'information**
   Mesure de la quantité d'information,
   Entropie, codage de l'information,
   Capacité du canal d'information.
3. **Présentation vectorielle des signaux**
   Notion d'espace vectoriel (norme, distance, espace de Hilbert)
   Produit scalaire et orthogonalité des signaux.
   Approximation des signaux,
4. **Analyse de Fourier**.
   Base de Fourier
   Séries de Fourrier, Transformation de Fourier
   Notion de spectre.
5. **Echantillonnage**
   Principe d'échantillonnage.
   Types d'échantillonnage (théorème de Shanon)
   Relations entre le spectre du signal et le spectre échantillonnée.
   Quantification.
   Notion de corrélation, de convolution, transformée en Z.
   Transformée de Fourier discrète.
   Transformée de Fourier rapide.

Références

1) Abedjalil Ouahabi , Traitement du signal, Théorie du signal, Signaux déterministes ,OPU 1987.
2) Christiane Rousseau, Yvan Saint-Aubin, Mathématiques et Technologie, 2008 Springer Science+ Business Media, LLC.
3) François Liret**,** MATHS EN PRATIQUE à l'usage des étudiants**,** Cours et exercices Dunod 2006.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 1

UEM1

Intitulé de la matière : Programmation Orientée Objet 1

Crédits : 5

Coefficients : 3

Objectifs de l'enseignement

Ce module consiste en premier à rappeler les principes de la programmation impérative et le langage C avant d'introduire la programmation orientée objet. Ce rappel permettra de bien montrer l'apport de la programmation orientée objet dans le développement de logiciels, et l'étude du langage de programmation JAVA largement utilisé dans l'industrie informatique, plus particulièrement dans les applications WEB.

Connaissances préalables recommandées

Algorithme et structures de données

Contenu de la matière

1- Rappel sur la programmation impérative
2- Langage C
3- Programmation Orientée Objet
   a. Motivations
   b. Notion d'objet
   c. Notion de classe
   d. Relation entre classe et objet
   e. Notion d'encapsulation
   f. Héritage et polymorphisme
4- Langage JAVA
   a. Objet
   b. Classe
   c. Héritage
   d. Swing
   e. Applets
   f. Servlets
   g. RMC et Threads

Références:

[1] Danny Poo, Derek Kiong et Swarnalatha Ashok. Object-Oriented Programming and JAVA. Second edition, Spring Verlag, 2008.

[2] James Gosling, Bill Joy, Guy Steele et Gilard Bracha. The Java Language Specification. Third Edition. Addition-Wesley. 2005.

[3] Stephen G. Kochan. Programming in C. Hayden Book Company, 1983.

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Semestre :1

UEM2

Intitulé de la matière : Introduction à la cryptographie.

Crédits : 4

Coefficients : 2

Objectifs de l'enseignement

Introduire les notions élémentaires de la cryptographie, étudier et analyser les cryptosystèmes classiques

Connaissances préalables recommandées

Module de l'algèbre 1 et l'algèbre 2, programmation

Contenu de la matière

1. Introduction
2. Aperçu historique, terminologie
3. Cryptographie invulnérable
4. Mécanismes de la cryptographie
5. Cryptographie conventionnelle
    a) Chiffrement par substitution
    b) Chiffrement par transposition
    c) Chiffrement de César
    d) Gestion des clés et cryptage conventionnel
6. Cryptographie de clé privée (symétrique)
    a) Exemples (DES, 3-DES, AES ; …)
7. Cryptographie de clé publique (asymétrique)
    a) Exemples (RSA ; Elgamel, …).
8. Protocoles de sécurité.
    a) Protocoles d'authentification
    b) Protocoles de distribution de clés
    c) Protocoles "zero knowledge"
9. Protocoles de commerce électronique

Références

1. Schneier Bruce, Cryptographie appliquée – Algorithmes, protocoles et code source en C. Tomson 1997.
2. Johannes A. Buchmann, Introduction to Cryptography, Springer 2000.
3. Menezes Alfred J., van Oorschot Paul C., Vanstone Scott A. Handbook of Applied Cryptographie. CRC Press LLC 1999.
4. Ireland & Rosen, *A Classical Introduction to Modern Number Theory*, Springer.
5. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994
6. Koblitz, *Algebraic Aspects of Cryptography*, Springer.
7. Schneier, *Cours de Cryptographie appliquée*, Wiley.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

UED1
Semestre *:* 1
Intitulé de la matière : Anglais **1**
Crédits : 2
Coefficients : 2

Objectifs de l'enseignement

Ce module a donc pour objectif de rendre l'étudiant d'avantage autonome dans son expression orale et écrite, ainsi que dans sa capacité à comprendre un document scientifique en langue anglaise

Connaissances préalables recommandées

Notions de la première année.

Contenu de la matière

1. *La première partie concerne un travail sur des documents récents lui permettent d'être au courant des dernières innovations du domaine de la haute technologie.*

2. *La deuxième partie du cours est consacrée aux documents déjà présenté. Ceci permet à l'étudiant de parfaire sa production orale. Des revues de presse hebdomadaires sont également présentées.*

Références *(Livres et polycopiés, sites internet, etc).*

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 1
UET1
Intitulé de la matière : Protection des systèmes d'exploitation
Crédits : 1
Coefficients : 1

Objectifs de l'enseignement

Ce cours permet à l'étudiant de connaitre la problématique du système d'exploitation (gestion et contrôle d'accès aux ressources), et d'acquérir une vision sur la protection du système contre des attaques internes et externes.

Connaissances préalables recommandées

Notions de la première année du tronc commun Mathématiques –Informatique.

Contenu de la matière

Partie I

1. Description du système d'exploitation
2. Rôles du système d'exploitation
3. Composantes du système d'exploitation
4. Systèmes multitâches
5. Systèmes multi-processeurs
6. Systèmes embarqués
7. Systèmes temps réel
8. Les types de systèmes d'exploitation

Partie II

Protection et sécurité

1. Authentification des utilisateurs
2. Attaques
   -Internes
   -Externes
3. Mécanismes de protections

Références

1. « Contribution à la sécurité des systèmes d'exploitation et des microprocesseurs » THESE `présentée et soutenue publiquement le 18 octobre 2007 pour l'obtention du Doctorat de l'université de Paris XI.
2. « Détection d'attaques dans un système WBAN de surveillance médicale à distance », Thèse de doctorat Présentée par Ali MAKKE Spécialité: Informatique et Réseaux Université Paris Descartes, Soutenue le 30 Mai 2014.

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 2

UEF1

Intitulé de la matière : Théorie des codes linéaires

Crédits : 6

Coefficients : 3

Objectifs de l'enseignement

L'objectif de ce cours est de familiariser l'étudiant avec les notions fondamentales des codes correcteurs d'erreurs, cette étude utilise les notions élémentaires d'algèbre linéaire. Cette matière a des applications en théorie de l'information et en cryptographie.

Connaissances préalables recommandées

Algèbre 1 et Algèbre 2.

Contenu de la matière

I) Rappel sur l'arithmétique

1. Congruences et Classes résiduelles, fonction Phi d'Euler.
2. Les Théorèmes de Fermat, Euler et de Lagrange
3. Résidualités quadratiques

II) Codes Linéaires

1.Introduction des codes linéaires.
2 Codes correcteurs d'erreurs.
3 Description par des matrices génératrices
4 Description par des matrices de contrˆole
5 Décodage d'un code linéaire, par le tableau standard, par le syndrome.
6. Codes duaux, codes auto-duaux.
7. Equivalence des codes, groupes d'automorphismes.

III). Exemples de codes linéaires

A) Codes de Hamming, décodage.
B) Codes de Hamming étendus
C) Codes de Reed Muller.
D) Codes cycliques
E) Codes BCH.
F) Codes de Goppa.

IV) Application des codes linéaires dans l'industrie

a) Code du disque compact.
b) Code des CD-Rom…..

Références

[1] J.H. van Lint, *Introduction to coding theory*, 3eme edition, Springer
[2] W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press 2003

[3]. F. Jessie MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977. Jürgen Bierbrauer.
[4]. *Introduction to Coding Theory*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, London, New York, Washington D.C., 2004.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 2
UEF1
Intitulé de la matière : Réseaux
Crédits : 6
Coefficients : 3

Objectifs de l'enseignement

L'objectif de ce cours est de donner aux étudiants de Master, des connaissances de base sur les réseaux. Ce cours présente les réseaux en général, puis passe à l'étude de TCP/IP avec quelques uns de ses mécanismes.

Connaissances préalables recommandées

Connaissances de la première année Licence.

Contenu de la matière :

1ère partie Principe des réseaux.

1.1 Introduction
1.2 Le modèle de référence OSI de l'ISO
1.3 La couche physique : Transmission en bande de base, transmission modulée, multiplexage et les supports de transmission
1.4 La couche liaison : Détection et correction d'erreurs et les protocoles de liaison de données
1.5 La couche réseau
  1.5.1 Le contrôle de flux
  1.5.2 Le problème de la congestion
  1.5.3 Le routage
1.6 La couche transport
1.7 Les couches hautes : session, présentation et application

2ème Partie : Le réseau Internet et les protocoles TCP/IP.

2.1 Architecture des protocoles TCP/IP
2.2 Adressage
2.3 La couche liaison
2.4 Le protocole IP
2.4.1 Le datagramme IP
2.4.2 La fragmentation des datagrammes IP
2.4.3 Le routage IP
2.4.4 La gestion des erreurs
2.5 Les protocoles TCP et UDP
2.5.1 Le protocole UDP
2.5.2 Le protocole TCP
2.6 Les applications (FTP, TFTP, Telenet, SMTP, HTTP, DHCP…)
2.7 Quelques commandes utiles

Références

1) Transmissions et réseaux, Cours et exercices corrigés. Stéphane Lohier, Dunod
2) Internetworking with TCP/IP, 4th edition, de Douglas COMER
3) Computer Networks, 4th edition, de Andrew S. TANENBAUM
4) High Speed Networks and Internets, 2nd edition, de William STALLINGS

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 2

UEF2

Intitulé de la matière : Complexité algorithmique et chiffrement.

Crédits : 6

Coefficients : 3

Objectifs de l'enseignement

L'objectif de ce module est de présenter les grands principes de la complexité algorithmique. Il s'agit de montrer les différentes classes de problèmes et la façon dont la complexité d'un algorithme est calculée afin d'analyser ses performances.

Connaissances préalables recommandées

Connaissances en programmation et en mathématiques du niveau Licence.

Contenu de la matière :

1. Introduction
2. Calcul de coût d'un algorithme
3. Complexité en temps et en espace
4. Machines de Turing
    a) Machines équivalentes.
    b) Machines de Turing non déterministes
    c) Machines de Turing universelles
5. Langage reconnu par une machine de Turing
6. Problème de décision.
7. Problèmes P, NP, NP-dur et autres.
    a) Le problème « Premier » est NP.
    b) Le problème de satisfaisabilité
    c) Le problème TSP
8. Algorithmes déterministes
9. Algorithmes probabilistes
10. Réduction et complétude
11. Théorie de la complexité et la cryptographie moderne.

Références

1) T. Cormen, C. Leiserson, R. Rivest. Introduction à l'algorithmique. Dunod, 1994
2) I. Lavallée, Complexité et algorithmique avancée - Une introduction. Hermann, 2008.
3) Christos H. Papadimitriou. Coputational complexity. Addison-Wesely. 1994
4) S. Arora, B. Barak. Computational complexity: A modern approach. Cambridge 2007

5) Douglas Stinson, *Cryptographie - Théorie et Pratique* (Vuibert, 2003)
6) Gilles Zemor : *Cours de Cryptographie* (Cassini, 2000)
7) Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1997)
8) Neal Koblitz, *A Course in Number Theory and Cryptography* (GTM 114, Springer, 1994)
9) Henri Cohen, *A course in computational algebraic number theory* (4 édition, GTM 138, Springer-Verlag, 2000)
10) Henri Cohen, *Advanced topics in computational number theory* (GTM 193, Springer-Verlag, 2000

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 2

UEM1

Intitulé de la matière : Programmation orientée objet 2

Crédits : 5

Coefficients : 3

Objectifs de l'enseignement

Dans ce module, on se concentre sur l'usage de la bibliothèque cryptographie, modèle de sécurité du langage JAVA. Le module sera illustré par un projet en petits groupes pour développer une application distribuée sécurisée.

Connaissances préalables recommandées

Programmation Orientée Objet et Génie Logiciel

Contenu de la matière

1. Modèles de développement de logiciel
    - Assemblage de composants
    - Modèle en spirale

2. Développement sécurisé
    - la définition d'une analyse de risque (identification des menaces, des hypothèses d'utilisation du produit, etc.) ;
    - les méthodes de mise en place de contre-mesures efficaces et exhaustives
    - les méthodes formelles ou semi-formelles (preuve de sécurité) ;
3. Langage Java et J2EE : utilisation de la bibliothèque Cryptographie de JAVA ; ainsi que le module de sécurité pour développer une application distribuée sécurisée.

Références:

[1] Danny Poo, Derek Kiong et Swarnalatha Ashok. Object-Oriented Programming and JAVA. Second edition, Spring Verlag, 2008.
[2] David . A. Gustafon. Theory and Problems of Software Engineering. Schaum's outline Series. McGRAW-HILL.2002 .
[3] James Gosling, Bill Joy, Guy Steele et Gilard Bracha. The Java Language Specification. Third Edition. Addition-Wesley. 2005.
[4] Heinz Zukkighoven. Object-Oriented Construction Handbook. Elsevier and dpunkt.verlag.2005.
[5] Stephen Gilbert et Bill Mc Carty. Object-Oriented Design in JAVA. 1998.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 2

UEM2

Intitulé de la matière : Calcul Formel

Crédits : 4

Coefficients : 2

Objectifs de l'enseignement

L'objectif de ce cours est de donner une introduction aux principaux éléments du calcul formel et d'utiliser le logiciel Maple pour résoudre des problèmes géométriques et algébriques. Le cours est accompagné d'un projet personnel.

Connaissances préalables recommandées

Connaissances en analyse, algèbre linéaire et géométrie du niveau Licence.

Contenu de la matière

1. Présentation des logiciels

1.1. Calcul formel versus calcul numérique.

1.2. Présentation générale de logiciels différents de calcul formel (Maple, Mathématica,).

2. Notions de base de calcul formel en Maple

2.1. Données et opérateurs

2.2. Symboles et variables

2.3. Expressions, évaluations et simplifications

2.4. Fonctions et procédures

2.5. Structures et opérations itératives

2.6. Conditionnement, programmation. Packages.

3. Domaines d'utilisation et applications

3.1. **Arithmétique**

3.1.1. Calculs entiers et rationnels

3.1.2. Divisibilité et primalité

3.1.3. Fractions continues

3.1.4. _Equations en nombres entiers

3.1.5 Applications de l'algorithme de Euclide.

3.2. **Calcul matriciel**

3.2.1. Matrices et vecteurs

3.2.2. Les objets vecteurs et matrice en Maple

3.2.3 Manipulation des matrices

3.2.4. Calculs matriciels de base

3.2.5. Résolution de systèmes linéaires

3.2.6. Calculs sur des matrices
3.2.7 Optimisation linéaire
3.2.8 Automatique
3.3. **Espaces vectoriels euclidiens**
3.3.1. Isométries
3.3.2. Réduction d'une forme quadratique
3.3.3. Optimisation quadratique
3.4 **Polynômes et fractions rationnelles**
3.4.1. Opérations purement syntaxiques
3.4,2 Récriture et simplification
3.4.3. Calculs en une variable
3.5. **Polynômes et systèmes multivariés**
3.5.1. Bases de Grobner
3.5.2. Applications
3.6. **Suites réelles**
3.6.1. Récurrences linéaires
3.6.2 Coeffi_cients constants
3.6.3 Coeff_cients polynomiaux
3.6.4 Récurrences d'ordre un
3.6.5 Récurrences du type un+1 = f(un)
3.6.6 Récurrences du type un+1 = f(n; un)

4. Projet personnel

Projet personnel pour la résolution d'un problème en algèbre, équations différentielles, géométrie différentielle.

Références

1. P. Fortin & R. Pomès, *Premiers pas en Maple,* Vuibert, 1995.

2. A. Leroux & R. Pomès, *Toutes les applications de Maple*, Vuibert, 1995.

3. Calcul formel, Mode d'emploi, exemples en Maple,
Philippe Dumas, Claude Gomez, Bruno Salvy, Paul Zimmermann Masson. 1995

4. Aho & Hopcroft & Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, 1994.

5. Bini & Pan, *Polynomial and matrix computations*, Birkhäuser, 1994.

6. Cox & Little & O'Shea, *Ideal, varieties and algorithms*, Springer.

7. von zur Gathen et Gerhard, *Modern Computer Algebra*, 2nd edition, Cambridge University Press, 2003

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Semestre *: 2*
UED1
Intitulé de la matière : Chiffrement audio
Crédits : 2
Coefficients : 2

Objectifs de l'enseignement

L'objectif de ce cours est de faire montrer à l'étudiant les dernières techniques utilisées dans le cryptage des fichiers audio. A l'issu de l'enseignement de cette matière, l'étudiant aura acquis des connaissances sur le cryptage de l'information audio et il va pouvoir programmer quelques algorithmes pour crypter et décrypter un fichier audio.

Connaissances préalables recommandées

- Basiques de la cryptographie.

Contenu de la matière

- Introduction
- Compression en MP3
- Chiffrement audio totale en utilisant DES
- Chiffrement audio totale en utilisant AES
- Chiffrement audio sélective en utilisant AES
- Chiffrement audio aléatoire (Audio shuffle encryption)

Références

[1] Chuck Easttom, *Modern Cryptography: Applied Mathematics for Encryption and Information Security,* McGraw-Hill Education; 1st edition (October 9, 2015).

[2] Shiguo Lian, *Multimedia content encryption,* CRC Press Taylor & Francis Group, 2009.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 2
UET1
Intitulé de la matière : Anglais **2**
Crédits : 1
Coefficients : 1

Objectifs de l'enseignement

Ce module a donc pour objectif de rendre l'étudiant d'avantage autonome dans son expression orale et écrite, ainsi que dans sa capacité à comprendre un document scientifique en langue anglaise

Connaissances préalables recommandées

Notions de la première année.

Contenu de la matière

1. *La première partie concerne un travail sur des documents récents lui permettent d'être au courant des dernières innovations du domaine de la haute technologie.*

2. *La deuxième partie du cours est consacrée aux documents déjà présenté. Ceci permet à l'étudiant de parfaire sa production orale. Des revues de presse hebdomadaires sont également présentées.*

Références

Mode d'évaluation : Continu et examen.

Intitulé du Master Cryptographie et Sécurité
Semestre *:* 3
UEF1
Intitulé de la matière Cryptographie avancée
Crédits : 6
Coefficients : 3
Objectifs de l'enseignement
Initier l'étudiant à l'étude des cryptosystèmes basés sur des problèmes algébriques ou des problèmes des codes correcteurs d'erreurs.
Connaissances préalables recommandées
Module de l'algèbre 1 et l'algèbre 2, module des corps finis, module des codes correcteurs d'erreurs.
Contenu de la matière
1. Introduction
- Besoins de sécurité
- Crypto-Systèmes Symétrique, Crypto-Systèmes Asymétrique
- Fonctions de Hachage
- Signature Électronique
- Nouvelles Tendances en Cryptographie
- Cryptanalyse

2. Chiffrement, sécurité.
- Fonction « one-way ».
- La méthode RSA et factorisation des entiers
- Logarithme discret et cryptosysteme d'El gamel
- La méthode du sac à dos.
- Codes correcteurs d'erreurs et cryptosystème de Mc Elièce.
- Courbes elliptiques, cryptosystemes
- Partage du secret.
- Cryptage d'images.
- Protection des droits d'auteurs.

3. Authentification
- Protocoles, Principes
- Techniques d'authentification, signature numérique.
- Signature à l'aide des clés publiques.
- Sécurité des fichiers.
- Algorithmes, exemples.

Références

1. Ireland & Rosen, *A Classical Introduction to Modern Number Theory*, Springer.
2. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994
3. Blake, Seroussi et Smart, *Elliptic Curves in Cryptography*, Springer.
4. Koblitz, *Algebraic Aspects of Cryptography*, Springer

Mode d'évaluation : Continu et examen

Intitulé du Master Cryptographie et Sécurité

Semestre *:* 3

UEF1

Intitulé de la matière : Sécurité informatique

Crédits : 7

Coefficients : 4

Objectifs de l'enseignement

Ce cours permet aux étudiants de dégager une compréhension globale et cohérente du domaine de la sécurité des réseaux informatiques, et être au fait des enjeux et des solutions techniques de la sécurité. Les étudiants apprendront des concepts fondamentaux de la sécurité des réseaux y compris l'analyse de vulnérabilités et les technologies utilisées pour la sécurité des réseaux. Des travaux pratiques seront réalisés pour consolider les concepts présentés durant le cours.

Connaissances préalables recommandées

Notions élémentaires d'informatiques.

Contenu de la matière

- Rappel sur les réseaux TCP/IP
- Aspects généraux de la sécurité
- Vulnérabilités des systèmes informatiques et méthodes d'attaque
  - Analyse de vulnérabilités
  - Attaques sur les protocoles réseau
  - Attaques sur les programmes
  - Attaques par code malicieux
  - Autres attaques
- Les système de filtrage de paquets (pare-feux)
  - Filtrage de paquets
  - Iptables/Netfilter
- Les systèmes de détection/prévention d'intrusion (IDS/IPS)

  La détection d'intrusion, NIDS/HIDS, Snort
- L'infrastructure à clé public (PKI)
- Les réseaux privés virtuels (VPN)
- Les protocoles de sécurité dans les réseaux IP
  - IPsec, TLS/SSL

Références

- Tableaux de bord de la sécurité réseau (2e édition) – Cédric Llorens, Laurent Levier Denis Valois, 2006.

- Transmissions et réseaux - 5ème édition - Cours et exercices corrigés. Stéphane Lohier et Dominique Présent. Dunond 2010
- Sécurité informatique : Principes et méthodes, Laurent Bloch , Christophe Wolfhugel , Nat Makarévitch. Eyrolles 2013
- Cryptography and Network Security: Principles and Practice, sixth Edition, William Stallings – Prentice Hall 2013

Mode d'évaluation : Continu et examen

Intitulé du Master Cryptographie et Sécurité

Semestre *:* 3

UEF1

Intitulé de la matière : Image et sécurité

Crédits : 5

Coefficients : 2

Objectifs de l'enseignement

L'objectif de ce module est d'introduire l'étudiant à travers l'utilisation de l'image dans les domaines d'application de sécurité suivants : recherche d'image, tatouage, reconnaissance faciale et reconnaissance d'empreinte.

Connaissances préalables recommandées

L'algèbre matriciel ;

Contenu de la matière

- Introduction au traitement d'image
- La recherche d'image par le contenu.
- Tatouage numérique d'image
- Reconnaissance faciale
- Détection d'empreinte.

Mode d'évaluation : *Contrôle continu + examen.*

Références

1. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker; "Digital Watermarking and Steganography" , 2nd Ed. Elsevier 2008.
2. Kresimir Delac, Mislav Grgic and Marian Stewart Bartlett; "Recent Advances in Face Recognition";2008 In-The.
3. Davide Maltoni, Dario Maio, Anil Jain, Salil Prabhakar ; « Handbook of Fingerprint Recognition" ; 2009 Springer.

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 3

UEM1

Intitulé de la matière : EDI et commerce électronique

Crédits : 5

Coefficients : 3

Objectifs de l'enseignement

Ce module a comme objectifs :

- La réalisation d'une une étude complète sur le commerce électronique dans un contexte B2B (échanges d'entreprise à entreprise) ou B2C (échanges d'entreprises à consommateurs).
- La sécurité dans le commerce électronique.

Connaissances préalables recommandées

Notions élémentaires d'informatiques.

Contenu de la matière :

1. Principes du e-business
    a) Stratégies
    b) Business models
    c) Systèmes d'information étendus
2. Plates-formes e-business
    a) sites commerciaux
    b) Catalogues en ligne
    c) Plates-formes d'achat
    d) Places de marché électronique
    e) Portails spécialisés
3. Modélisation des processus et rôle des progiciels intégrés (ERP, CRM…) ;
4. Commerce électronique B2B
    a) Etat de l'art EDI
    b) Initiation UML/XML
    c) Web-EDI
5. Sécurité et paiement électronique.
6. Sécurité des agents mobiles
7. Sécurité du commerce mobile
8. Sécurité de la carte à puce

Références:

[1] Wil van der Aalst et Kees van Hee. Workflow Management : Models , Methods and Systems. The MIT Press Cambridge Massachusetts London, England. 2002.

[2] E-Business Innovation and Process Management. In Lee, Western Illinois University, USA, Cybertech Publishing 2007.

[3] Vesna Hassler. Security Fundamentals for E-Commerce. Artech House INC,

2001.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 3

UEM1

Intitulé de la matière : Sûreté de fonctionnement des systèmes informatiques

Crédits : 4

Coefficients : 2

Objectifs de l'enseignement

Maîtriser les bases théoriques de la sureté de fonctionnement des systèmes informatiques indépendamment du matériel employé, mettre en pratique les techniques d'évitement, de suppression et de tolérances aux fautes.

Connaissances préalables recommandées

Notions élémentaires d'informatiques.

Contenu de la matière

1, Problématique de la sureté de fonctionnement des systèmes informatiques
2. Mécanismes destructeurs.
3. Les défaillances et leurs causes
4. Définitions des fautes et de leurs effets
5. Modèles de fautes des technologies matérielles et logicielles.
6. Mécanismes protecteurs
7. Evaluation de la sûreté de fonctionnement
8. La redondance
9. Les codes détecteurs et correcteurs d'erreurs.
10. Panorama des méthodes de protection.
11. Test en ligne
12. Systèmes à défaillances non dangereuses.
13. Synthèse comparative.

Références

1. Sureté de fonctionnement des systèmes informatiques, Jean- Claude Geffroy, Gilles Motet, InterEditions. 1998.
2. Spécification et conception des systèmes, une méthodologie, J .P. Calver, Masson Editeur. 1992.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 3
UED1
Intitulé de la matière : Méthodologie de la recherche
Crédits : 2
Coefficients : 2

Objectifs de l'enseignement

Permettre aux étudiants de s'initier aux principales méthodes de recherche, de mener correctement un projet de recherche, et de savoir communiquer les résultats de la recherche.

Connaissances préalables recommandées

Contenu de la matière :

- *La recherche publique et en entreprise*
- *Méthodes de recherche*
- *L'évaluation de la recherche*
- *Les outils d'un chercheur*
- *Communication des résultats de la recherche.*

Références

1. Dalhoumi S. « Cours de méthodologie », support de cours, Formation de formateurs, Cerist, Alger, Février 2004.
2. Labasse B., « La communication scientifique ; principes et méthodes », Pôle Universitaire de Lyon, 2001
3. Mucchielli A., « La nouvelle communication : épistémologie des sciences de l l'information – communication », Armand Collin, 2000
4. Salvador Juan. « Méthodes de recherche en sciences socio-humaines : Approche critique des techniques », Presses Universitaires de France (PUF), 1999, p304.

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Semestre *:* 3
UET1
Intitulé de la matière : Ethique et déontologie
Crédits : 1
Coefficients : 1

Objectifs de l'enseignement

Dispenser dans le cadre de ce cours les principes qui régissent le comportement des différents acteurs de l'enseignement supérieurs. Un accent particulier sera mis sur l'éthique en matière de publication de papiers scientifique.

Connaissances préalables recommandées

Notions de la première année.

Contenu de la matière

1. *Introduction*
2. *Science et éthique*
3. *Les valeurs sociales*
4. *Les valeurs professionnelles*
5. *Les valeurs individuelles*
6. *Ethique dans l'enseignement supérieur*
7. *Ethique dans la publication de papiers de recherche*

Références

- *IEEE ethics in paper publishing , www.IEEE.org*

Mode d'évaluation : Continu et examen.

V- Accords ou conventions

Oui

NON

(Si oui, transmettre les accords et/ou les conventions dans le dossier papier de la formation)

LETTRE D'INTENTION TYPE

(En cas de master coparrainé par un autre établissement universitaire)

(Papier officiel à l'entête de l'établissement universitaire concerné)

Objet : Approbation du coparrainage du master intitulé :

Par la présente, l'université (ou le centre universitaire) déclare coparrainer le master ci-dessus mentionné durant toute la période d'habilitation de ce master.

A cet effet, l'université (ou le centre universitaire) assistera ce projet en :

- Donnant son point de vue dans l'élaboration et à la mise à jour des programmes d'enseignement,

- Participant à des séminaires organisés à cet effet,
- En participant aux jurys de soutenance,
- En œuvrant à la mutualisation des moyens humains et matériels.

SIGNATURE de la personne légalement autorisée :

FONCTION :

Date :

LETTRE D'INTENTION TYPE

(En cas de master en collaboration avec une entreprise du secteur utilisateur)

(Papier officiel à l'entête de l'entreprise)

OBJET : Approbation du projet de lancement d'une formation de master intitulé :

Dispensé à :

Par la présente, l'entreprise déclare sa volonté de manifester son accompagnement à cette formation en qualité d'utilisateur potentiel du produit.

A cet effet, nous confirmons notre adhésion à ce projet et notre rôle consistera à :

- Donner notre point de vue dans l'élaboration et à la mise à jour des programmes d'enseignement,
- Participer à des séminaires organisés à cet effet,
- Participer aux jurys de soutenance,
- Faciliter autant que possible l'accueil de stagiaires soit dans le cadre de mémoires de fin d'études, soit dans le cadre de projets tuteurés.

Les moyens nécessaires à l'exécution des tâches qui nous incombent pour la réalisation de ces objectifs seront mis en œuvre sur le plan matériel et humain.

Monsieur (ou Madame)……est désigné(e) comme coordonateur externe de ce projet.

SIGNATURE de la personne légalement autorisée :

FONCTION :

Date :

CACHET OFFICIEL ou SCEAU DE L'ENTREPRISE