REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

NOUVELLE
OFFRE DE FORMATION MASTER

ACADEMIQUE

Etablissement	Faculté	Département

Domaine : Mathématiques & Informatique.
Filière : Informatique.
Spécialité : Sécurité informatique.

Année universitaire : 2025 / 2026.

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

عرض تكوين جديد
ماستر
أكاديمي

المؤسسة	الكلية/ المعهد	القسم

الميدان : رياضيات و إعلام آلي

الشعبة : إعلام آلي

التخصص : أمن معلوماتي

السنة الجامعية: 2025/ 2026

II– Fiche d’organisation semestrielle des enseignements.

Spécialité : Sécurité Informatique .

السداسي 1:

وحدة التعليم	عنوان المواد	الرصيد	المعامل	الحجم الساعي الأسبوعي			الحجم الساعي للسداسي (14 أسبوع)	أخرى	نوع التقييم	
				دروس	أعمال موجهة	أعمال تطبيقية			مراقبة مستمرة	امتحان
وحدة تعليم أساسية **الرمز: وت أس 1.1.1** **الأرصدة: 10** **المعامل: 6**	الخوارزميات المتقدمة والتعقيد	5	3	1سا30	1سا30	1سا30	63سا00	42سا00	40%	60%
	قواعد البيانات المتقدمة	5	3	1سا30	1سا30	1سا30	63سا00	42سا00	40%	60%
وحد تعليم أساسية **الرمز: وت أس 1.1.2** **الأرصدة: 8** **المعامل: 6**	الأدوات الرياضية للتشفير	4	4	1سا30	1سا30	1سا30	63سا00	42سا00	40%	60%
	الذكاء الاصطناعي للأمن السيبراني	4	2	1سا30	-	1سا30	42سا00	21سا00	40%	60%
وحدة تعليم منهجية **الرمز: وت م 1.1** **الأرصدة: 9** **المعامل: 4**	مقدمة في أمن الحاسوب	5	2	1سا30	1سا30	-	42سا00	21سا00	40%	60%
	الاختراق الأخلاقي ودفاع النظام	4	2	1سا30	-	1سا30	42سا00	21سا00	40%	60%
وحدة تعليم أفقية **الرمز: وت أف 2.2** **الأرصدة: 2** **المعامل: 1**	تطوير وعمليات (DevOps)	2	1	1سا30	-	1سا30	42سا00	21سا00	40%	60%
وحدة تعليم استكشافية **الرمز: وت إس 1.1** **الأرصدة: 1** **المعامل: 1**	مادة للإختيار	1	1	1سا30	-	-	21سا00	21سا00	-	100%
مجموع السداسي 1		**30**	**18**	**12سا00**	**6سا00**	**9سا00**	**378سا00**	**231سا00**		

ا

السداسي 2:

وحدة التعليم	عنوان المواد	الرصيد	المعامل	الحجم الساعي الأسبوعي			الحجم الساعي للسداسي (14 أسبوع)	أخرى	نوع التقييم	
				دروس	أعمال موجهة	أعمال تطبيقية			مراقبة مستمرة	امتحان
وحدة تعليم أساسية **الرمز: وت أس 1.2.1** **الأرصدة: 9** **المعامل: 6**	التشفير والأمن	5	3	1سا30	1سا30	1سا30	63سا00	42سا00	40%	60%
	أمن وتحليل جنائي لقواعد البيانات	4	3	1سا30	-	1سا30	42سا00	21سا00	40%	60%
وحد تعليم أساسية **الرمز: وت أس 1.2.2** **الأرصدة: 9** **المعامل: 6**	الشبكات المتقدمة والأمن	5	3	3سا00	1سا30	1سا30	84سا00	42سا00	40%	60%
	الجرائم الإلكترونية	4	3	1سا30	-	1سا30	42سا00	21سا00	40%	60%
وحدة تعليم منهجية **الرمز: و ت م 1.2** **الأرصدة: 9** **المعامل: 4**	أمن الوسائط المتعددة والتحقيق الجنائي	4	2	1سا30	-	1سا30	42سا00	21سا00	40%	60%
	أمن إنترنت الأشياء	5	2	1سا30	-	1سا30	42سا00	21سا00	40%	60%
وحدة تعليم أفقية **الرمز: وت أف 1.2** **الأرصدة: 2** **المعامل: 1**	إدارة مشاريع المعلوماتية	2	1	1سا30	-	1سا30	42سا00	21سا00	40%	60%
وحدة تعليم استكشافية **الرمز: وت إس 1.1** **الأرصدة: 1** **المعامل: 1**	مادة للإختيار	1	1	1سا30	**-**	**-**	21سا00	21سا00	**-**	100%
مجموع السداسي 2		**30**	**18**	**13سا30**	**3سا00**	**10سا30**	**378سا00**	**210سا00**		

السداسي 3:

وحدة التعليم	عنوان المواد	الرصيد	المعامل	الحجم الساعي الأسبوعي			الحجم الساعي للسداسي (14 أسبوع)	أخرى	نوع التقييم	
				دروس	أعمال موجهة	أعمال تطبيقية			مراقبة مستمرة	امتحان
وحدة تعليم أساسية **الرمز: وت أس 1.1.1** **الأرصدة: 9** **المعامل: 6**	أمن أنظمة التشغيل	4	3	1سا30	1سا30	1سا30	63سا00	42سا00	40%	60%
	الافتراضية، الحوسبة السحابية، والأمن	5	3	1سا30	-	3 سا00	63سا00	42سا00	40%	60%
وحد تعليم أساسية **الرمز: وت أس 1.1.2** **الأرصدة: 9** **المعامل: 6**	المصادقة والتحكم في الوصول	5	3	1سا30	1سا30	1سا30	63سا00	42سا00	40%	60%
	أمن تطبيقات الويب و تطبيقات الهواتف المحمولة	4	3	1سا30	-	1سا30	42سا00	21سا00	40%	60%
وحدة تعليم منهجية **الرمز: وت م 1.1** **الأرصدة: 9** **المعامل: 4**	الأدلة الجنائية الرقمية	4	2	1سا30	-	1سا30	42سا00	21سا00	40%	60%
	برمجة وسلامة الأنظمة الموزعة	5	2	1سا30	1سا30	1سا30	63سا00	42سا00	40%	60%
وحدة تعليم أفقية **الرمز: وت أف 1.2** **الأرصدة: 2** **المعامل: 1**	منهجية البحث	2	1	1سا30	-	-	21سا00	21سا00	-	100%
وحدة تعليم استكشافية **الرمز: وت إس 1.1** **الأرصدة: 1** **المعامل: 1**	مادة للإختيار	1	1	1سا30	-	-	21سا00	21سا00	-	100%
مجموع السداسي 3		**30**	**18**	**12سا00**	**4سا30**	**10سا30**	**378سا00**	**252سا00**		

1- Semestre 1.

Unités d'Enseignement	VHS	VH Hebdomadaire				Coeff.	Crédits	Mode d'évaluation	
	14 Sem.	Cours	TD	TP	Travail Personnel			Continu	Examen
Unité d'Enseignement Fondamentale (UEF)						**12**	**18**		
UEF11 :	**126h**	**3h**	**3h**	**3h**	**6h**				
Algorithmique avancée et complexité		1h30	1h30	1h30	3h	3	5	40%	60%
Bases de données avancées		1h30	1h30	1h30	3h	3	5	40%	60%
UEF12 :	**105h**	**3h**	**1h30**	**3h**	**4h30**				
Outils mathématiques pour la cryptographie		1h30	1h30	1h30	3h	3	4	40%	60%
Intelligence artificielle pour la cybersécurité		1h30		1h30	1h30	3	4	40%	60%
Unité d'Enseignement Méthodologique (UEM)						**4**	**9**		
UEM1 :	**84h**	**3h**	**1h30**	**1h30**	**3h**				
Introduction à la sécurité informatique		1h30	1h30		1h30	2	5	40%	60%
Piratage éthique et défense des systèmes		1h30		1h30	1h30	2	4	40%	60%
Unité d'Enseignement Transversale (UET)						**1**	**2**		
UET1 :	**42h**	**1h30**		**1h30**	**1h30**				
DevOps		1h30		1h30	1h30	1	2	40%	60%
Unité d'Enseignement Découverte (UED)						**1**	**1**		
UED1 :	**21h**	**1h30**			**1h30**				
Matière au choix		1h30			1h30	1	1		100%
Total Semestre 1	**378h**	**12h**	**6h**	**9h**	**16h30**	**18**	**30**		

2- Semestre 2.

Unités d'Enseignement	VHS	VH Hebdomadaire				Coeff.	Crédits	Mode d'évaluation	
	14 Sem.	Cours	TD	TP	Travail Personnel			Continu	Examen
Unité d'Enseignement Fondamentale (UEF)						**12**	**18**		
UEF21 :	**105h**	**3h**	**1h30**	**3h**	**4h30**				
Cryptographie et sécurité		1h30	1h30	1h30	3h	3	5	40%	60%
Sécurité et criminalistique des bases de données		1h30		1h30	1h30	3	4	40%	60%
UEF22 :	**126h**	**4h30**	**1h30**	**3h**	**4h30**				
Réseaux avancés et sécurité		3h	1h30	1h30	3h	3	5	40%	60%
Cybercriminalité		1h30		1h30	1h30	3	4	40%	60%
Unité d'Enseignement Méthodologique (UEM)						**4**	**9**		
UEM2 :	**84h**	**3h**		**3h**	**3h**				
Forensiques multimédia et sécurité		1h30		1h30	1h30	2	4	40%	60%
Sécurité de l'IoT		1h30		1h30	1h30	2	5	40%	60%
Unité d'Enseignement Transversale (UET)						**1**	**2**		
UET2 :	**42h**	**1h30**		**1h30**	**1h30**				
Gestion de projets informatiques		1h30		1h30	1h30	1	2	40%	60%
Unité d'Enseignement Découverte (UED)						**1**	**1**		
UED2 :	**21h**	**1h30**			**1h30**				
Matière au choix		1h30			1h30	1	1		100%
Total Semestre 2	**378h**	**13h30**	**3h**	**10h30**	**15h**	**18**	**30**		

3- Semestre 3.

Unités d'Enseignement	VHS	VH Hebdomadaire				Coeff.	Crédits	Mode d'évaluation	
	14 Sem.	Cours	TD	TP	Travail Personnel			Continu	Examen
Unité d'Enseignement Fondamentale (UEF)						**12**	**18**		
UEF31 :	**126h**	**3h**	**1h30**	**4h30**	**6h**				
Sécurité des systèmes d'exploitation		1h30	1h30	1h30	3h00	3	4	40%	60%
Virtualisation, Cloud Computing et sécurité		1h30		3h	3h00	3	5	40%	60%
UEF32 :	**105h**	**3h**	**1h30**	**3h**	**4h30**				
Authentification et contrôle d'accès		1h30	1h30	1h30	3h00	3	5	40%	60%
Sécurité des applications Web et mobiles		1h30		1h30	1h30	3	4	40%	60%
Unité d'Enseignement Méthodologique (UEM)						**4**	**9**		
UEM3 :	**105h**	**3h**	**1h30**	**3h**	**4h30**				
Criminalistique numérique		1h30		1h30	1h30	2	4	40%	60%
Programmation et sûreté des systèmes répartis		1h30	1h30	1h30	3h	2	5	40%	60%
Unité d'Enseignement Transversale (UET)						**1**	**2**		
UET3 :	**21h**	**1h30**			**1h30**				
Méthodologie de recherche		1h30			1h30	1	2		100%
Unité d'Enseignement Découverte (UED)						**1**	**1**		
UED3 :	**21h**	**1h30**			**1h30**				
Matière au choix		1h30			1h30	1	1		100%
Total Semestre 3	**378h**	**12h00**	**4h30**	**10h30**	**18h**	**18**	**30**		

4- Semestre 4.

Domaine **:** Mathématiques et Informatique.
Filière **:** Informatique.
Spécialité **:** Sécurité Informatique .

	VHS	Coeff.	Crédits
PFE avec Mémoire	750 h	18	30
Stage dans l'entreprise			
Ateliers			
Travail Personnel			
Autres			
Total Semestre 4	**750 h**	**18**	**30**

5- Récapitulatif global de la formation.

UE → / VH	UEF	UEM	UET	UED	S4	Total
Cours	273 h	126 h	63 h	63 h		525 h
TD	147 h	42 h	-	-		189 h
TP	273 h	105 h	42 h	-		420 h
Mémoire	-	-	-	-	750 h	750 h
Stage dans l'entreprise	-	-	-	-		-
Ateliers	-	-	-	-		-
Travail Personnel	420 h	147	63 h	63 h		693 h
Autres	-	-	-	-		-
Total	1113 h	420 h	168 h	126 h	750 h	**2577 h**
Crédits	54	27	6	3	30	**120**
% en crédits pour chaque UE	45%	22.50%	5%	2.50%	25%	100%

Corbeille des modules de découverte au choix (UED)

- Informatique verte
- Gouvernance et transformation digitale
- Philosophie des sciences et de la technologie
- Droit du numérique et protection des données (RGPD)
- Psychologie cognitive
- Technologies émergentes (Blockchain, IOT, …)
- Découverte des spécialités de master (une première partie qui permet de découvrir sommairement les autres spécialités du master et une seconde partie qui permet de découvrir en détails les applications potentielles de la spécialité en cours)……

Liste des modules communs entre les spécialités

		STANDARS							SPECIFIQUES
#	MODULES / SPECIALITES	IF	GL	ISI	SD	IA	SEI	RSD	.....
1	Algorithmique Avancée & Complexité	X	X	X	X	X	X	X	X
2	Bases de Données Avancées	X	X	X	X	X	X	X	X
3	Ingénierie des Exigences		X	X					
4	Machine Learning (UEF)				X	X			X
5	Méthodes de Conception de log & Design Patterns	X	X	X					X
6	Analyse de données			X	X	X		X	
7	Paradigmes de Programmation	X	X						X
8	Méthodes d'optimisation					X			X
9	Réseaux avancés	X	X	X	X	X			X
10	DevOps						X		X
11	Deep Learning					X			X
12	Big data Analytics				X				X
13	Vision par ordinateur					X			X
14	Systèmes d'information coopératifs		X	X					
15	Sémantiques Formelle des Langages de Prog	X	X						
16	Systèmes Multi-Agents	X	X						
17	Machine learning (UEM)	X	X	X				X	X
18	Virtualisation et Cloud Computing				X	X			
19	Gestion des projets informatiques	X	X	X	X	X	X	X	X
20	Intelligence artificielle générative					X			X
21	Virtualisation, Cloud Computing et sécurité						X	X	
22	Ingénierie Dirigée par les Modèles	X	X						
23	Spécification et Vérification Formelle	X	X						
24	Reconnaissance des formes					X			X
25	Modélisation et éval des performances des syst.	X	X						
26	Natural Language Processing				X	X			
27	Méthodologies de recherche	X	X	X	X	X	X	X	X

III - Programme détaillé par matière.

Spécialité : Sécurité Informatique .

Intitulé du master : Sécurité informatique .

Semestre : S1.

UE : UEF111.

Titre de la matière : Algorithmique avancée et complexité.

Crédit : 5.

Coefficient : 3.

Objectifs de la matière : Cette matière couvre des concepts fondamentaux et des techniques avancées en conception et analyse d'algorithmes en approfondissant les structures de données, les algorithmes de recherche et de tri, ainsi que des approches comme la programmation dynamique et les algorithmes gloutons. Elle fournit aussi une compréhension approfondie de la complexité algorithmique, en mettant l'accent sur les techniques d'analyse, l'importance de la complexité pour l'optimisation et les méthodes pour prouver la correction des algorithmes.

Connaissances préalables recommandées : Algorithmique, structures de données avancées et programmation.

Contenu de la matière :

1- Introduction à la complexité algorithmique et notions préliminaires.
- Définition d'algorithme et d'algorithmique.
- Notion de problème algorithmique et sa résolution.
- Pourquoi analyser la complexité ? Comparaison d'algorithmes pour un même problème.
- Notions de base et types de complexité : temporelle et spatiale.

2- Analyse de la complexité temporelle.
- Notation grand O (O) : Définition, interprétation et utilité pour exprimer la complexité asymptotique.
- Calcul de la complexité.
  - Identification des opérations élémentaires (comparaisons, affectations, etc.).
  - Analyse des boucles et des fonctions récursives.
  - Cas le pire, le meilleur, et moyen.
  - Exemples de complexités courantes : O(1), O(log n), O(n), O(n log n), O(n^2), etc.

3- Structures de données et complexité.
- Tableaux, listes chaînées, arbres, graphes, Tas : opérations courantes et complexité associée.
- Impact de la structure de données sur la complexité d'un algorithme.

4- Techniques d'analyse de complexité.
- Diviser pour régner : Stratégie de base, analyse de la complexité (exemple, tri par fusion).
- Programmation dynamique : Principe et optimisation (exemples : problème du sac à dos, plus court chemin).
- Algorithmes gloutons : Principes et analyse de la complexité. (Exemples voyageur de commerce, algorithme de Djikstra).

5- Complexité spatiale.
- Mesure de l'utilisation de la mémoire par un algorithme.
- Lien avec la complexité temporelle et compromis possibles.

6- Complexité et Preuve de Correction.
  - Notions de P, NP, NP-complet : Définitions et exemples de problèmes NP-complets.
  - Techniques de Preuve de Correction : Preuve par induction, preuves par contradiction.

7- Optimisation d'algorithmes.
- Utilisation des concepts de complexité pour identifier les points faibles d'un algorithme.

Techniques d'optimisation (par exemple, simplification de boucles, réduction de la récursivité).

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein (2009). Introduction to Algorithms. MIT Press, 3rd Edition.
2. Ivan Lavallée (2008). Complexité et algorithmique avancée : une introduction. Editions Hermann.
3. Jon Kleinberg, Éva Tardos (2005). Algorithm Design. Pearson Publisher, 1st edition.
4. Nicolas Hermann et Pierre Lescanne (2005). Est-ce que P = NP ? Les Dossiers de La Recherche, 20 : 64–68, août-octobre.
5. Robert Sedgewick, Kevin Wayne (2011). Algorithms, Addison-Wesley, 4th edition.
6. Förg Flum, Martin Grohe. Parameterized Complexity Theory. Springer Verlag, 2006.
7. Udi Manber 1989). Introduction to Algorithms: A Creative Approach. Addison-Wesley.
8. J. J. McConnell (2001). Analysis of algorithms: an active learning approach. Jones and Barlett Publishers.
9. Cormen, Leiserson, Rivest Stein (2010). Algorithmique, cours exercices et problèmes, 3ème édition, Dunod.
10. Sylvain Perifel (2014). Complexité algorithmique. Ellipses.
11. -Sanjeen Arora and Boaz Barak (2006). Computational Complexity: A Modern Approach.

Intitulé du master : Sécurité informatique .

Semestre : S1.

UE : UEF112.

Titre de la matière : Base de données avancée.

Crédit : 5.

Coefficient : 3.

Objectifs de la matière : Cette matière, en l'accent sur les concepts et technologies essentiels pour la conception, la gestion et l'exploitation de systèmes de bases de données modernes, en abordant à la fois les aspects théoriques et pratiques, permet à l'étudiant d'actualiser et d'approfondir ses connaissances des bases de données.

Connaissances préalables recommandées : Concepts de bases sur les bases de données, Langage SQL, Algèbre relationnelle.

Contenu de la matière :

1- Introduction aux bases de données.
   - Rappels sur les concepts fondamentaux : Modèle relationnel, SGBD, langages de requêtes.
   - Types de bases de données : Relationnelles, NoSQL, objets, etc.
   - Architecture d'un SGBD : Client-serveur, architectures distribuées.
   - Concepts de transaction, concurrence, et récupération de données.

2- Programmation SQL avancée.
   - SQL avancé : Jointures, sous-requêtes, fonctions d'agrégation, vues, procédures stockées.
   - Les Triggers.
   - Les fonctions et procédures stockées.
   - Traitement et gestion des erreurs.
   - Langages de manipulation de données pour NoSQL : JSONiq, Cypher.

3- Le modèle Objet-Relationnel.
   - Présentation du modèle Objet.
   - Présentation du modèle Relationnel-Objet.
   - Concepts du modèle RO (types complexes, héritage…).
   - Interrogation des BDD Relationnelles-Objet (SQL3).

4- Bases de données NoSQL.
   - Introduction aux bases de données NoSQL : Types de bases de données (clés-valeurs, documents, graphes, colonnes).
   - Modèles de données NoSQL : Avantages et inconvénients.
   - Études de cas : MongoDB, Cassandra, Neo4j.

5- Bases de données distribuées.
   - Architecture des systèmes distribués.
   - Techniques de réplication et de partitionnement.
   - Consistance des données dans un environnement distribué : ACID vs BASE.

6- Bases de données dans le Cloud.
   - Modèles de service : IaaS, PaaS, SaaS.
   - Cloud Computing et bases de données.
   - Considérations de sécurité dans le Cloud.

7- Performance et sécurité des bases de données.
   - Optimisation des requêtes SQL.
   - Indexation et stratégies d'accès.
   - Sécurité : Contrôle d'accès, chiffrement des données, audit.

- Gestion de la sécurité dans les bases de données distribuées.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. R. Elmasri & S. Navathe (2016). Fundamentals of Database Systems, 7th Edition, Pearson.
2. R. Elmesri, B. Navate (2016). Fundamentals of Database Systems. 7th edition, Pearson Editions.
3. T. Connolly & C. Begg (2014). Database Systems: A Practical Approach to Design, Implementation, and Management, 6th Edition, Pearson.
4. Christian Soutou (2013). SQL pour Oracle. Editions Eyrolles.
5. Silberschatz, H. Korth & S. Sudarshan (2019). Database System Concepts, 7th Edition, McGraw-Hill.
6. Mohamed Fadhel SAAD (2016). PL/SQL sous Oracle 12c. Guide du développeur.
7. R.G.G. Cattell (1994). Object Data Management. Addison-Wesley.
8. P. Selmer (2012). NOSQL stores and Data analytics tools. Advances in Data Management.
9. Christopher Diaz, Database Security: Problems and Solutions, Mercury Learning and Information, 2022.

Intitulé du master : Sécurité informatique .

Semestre : S1.

UE : UEF121.

Titre de la matière : Outils mathématiques pour la cryptographie.

Crédit : 4.

Coefficient : 3.

Objectifs de la matière : La première partie introduit les notions fondamentales de la théorie des groupes, notions utiles à la compréhension des corps et des codes linéaires ainsi que de leurs applications. La seconde partie doit permettre à l'étudiant d'acquérir les connaissances élémentaires apportées par la théorie des corps finis.

Connaissances préalables recommandées : Quelques notions d'algèbre.

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 spéciaux.
7. Groupes de permutations, groupes de matrices.
8. Exemples d'applications en cryptographie.

Partie 2.

1. Définitions, caractéristiques, cardinalité d'un corps fini.
2. Relation de Frobenius, morphisme de Frobenius.
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, théorèmes de Fermat, d'Euler et de Lagrange.
9. Résidu quadratique.
10. Suites récurrentes et registre à décalage.
11. Exemples d'application : clés cryptographiques.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. J. Querre, Cours d'algèbre, Maîtrise 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 : Sécurité informatique .

Semestre : S1.

UE : UEF122.

Titre de la matière : Intelligence artificielle pour la cybersécurité.

Crédit : 4.

Coefficient : 3.

Objectifs de l'enseignement : Cette matière permet à l'étudiant d'aborder les technologies et les sujets avancés de l'IA, couvrant diverses méthodes d'IA et leurs applications en cybersécurité. Il présente également des exemples d'applications d'algorithmes d'IA pour résoudre des problèmes de cybersécurité. Python est le langage principal du cours, mais certains projets peuvent inclure d'autres langages et outils.

Connaissances préalables recommandées : /.

Contenu de la matière :

1. Quelques définitions.
2. Une courte histoire de l'IA.
3. Grands domaines de l'IA.
4. Recherche informée : Recherche A* et heuristique.
5. Agents intelligents.
6. Apprentissage automatique et apprentissage profond.
   a. Modèles d'apprentissage supervisé et non supervisé.
   b. Création d'un pipeline d'apprentissage automatique.
   c. Apprentissage profond.
7. Introduction à l'apprentissage par renforcement.
8. Incertitude et raisonnement probabiliste.
9. Applications de l'IA en cybersécurité.
   a. Aperçu des applications de l'IA en cybersécurité (problèmes de confidentialité des données).
   b. Sécurité informatique et réseaux pilotés par les données (Data-Driven Network).
   c. Méthodes de filtrage anti-spam.
   d. Applications de l'apprentissage automatique à la sécurité des réseaux.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Stuart Russel and Peter Norvig, Artificial Intelligence: A Modern Approach, Prentice Hall Series in Artificial Intelligence, 2003.
2. Antoine Cornuéjols et Laurent Miclet, Apprentissage artificiel - Concepts et algorithmes -, EYROLLES, 2010.
3. Virginie MATHIVET, l'Intelligence artificielle pour les développeurs - Concepts et implémentations en Java, EYROLLES, 2015.
4. Hands-On Artificial Intelligence for Cybersecurity (Parisi et al, Packt Publishing, 2019).
5. Practical AI for Cybersecurity (Ravi Das, CRC Press, 2021).
6. Machine Learning and Security, (David Freeman, Clarence Chio), O'Reilly Media, Inc., 2018. (electronic edition available via MQ Library).

Intitulé du master : Sécurité informatique .

Semestre : S1.

UE : UEM111.

Titre de la matière : Introduction à la sécurité informatique.

Crédit : 5.

Coefficient : 2.

Objectifs de l'enseignement : Le but de cette matière est de présenter les différents aspects reliés à la sécurité informatique. De plus, il permet l'introduction d'un langage de script.

Connaissances préalables recommandées : /.

Contenu de la matière :

Chapitre 1 : Prise d'informations.

1. Prise d'informations à distance sur des réseaux d'entreprise et des systèmes distants.
2. Informations publiques.
3. Localiser le système cible.
4. Enumération des services actifs.

Chapitre 2 : Attaques à distance.

1. Intrusion à distance des postes clients par exploitation des vulnérabilités sur les services distants et prise de contrôle des postes utilisateurs par troyen.
2. Authentification par brute force.
3. Recherche et exploitation de vulnérabilités.
4. Prise de contrôle à distance.

Chapitre 3 : Attaques systèmes.

1. Attaques du système pour outrepasser l'authentification et/ou surveiller l'utilisateur suite à une intrusion.
2. Attaque du Bios.
3. Attaque en local.
4. Cracking de mot de passe.
5. Espionnage du système.

Chapitre 4 : Se sécuriser.

1. Outils de base permettant d'assurer le minimum de sécurité à son S.I.
2. Cryptographie.
3. Chiffrement des données.
4. Détection d'activité anormale.
5. Initiation à la base de registre.
6. Firewalling.
7. Anonymat.

Chapitre 5: Script.

1. Anonymat.
2. Introduction.

3. Emplacement d’un code Script.
4. Écriture d'un programme Script.
5. Les éléments de base d’un langage Script.
6. Étude des objets Script.
7. La boîte à outils.

Mode d’évaluation : Contrôle continu et Examen.

Références bibliographiques :

1. Robin Sharp. Introduction to Cybersecurity, Springer Nature Switzerland, 2023.
2. Nuno Mateus-Coelho, Maria Manuela Cruz-Cunha. Contemporary Challenges for Cyber Security and Data Privacy, IGI Global, 2023.
3. Hacking, Emmanuel Vinatier, Micro Application, 2004.
4. Charles P. Pfleege et Shari Lawrence Pfleege. Security in Computing, Prentice Hall PTR, 2003.
5. JavaScript Volume 2208 Le Guide complet, Olivier ondermarck, MA éditions, 2009.
6. JavaScript : Des fondamentaux aux concepts avancés, Emmanuel Gutierrez, Ediciones ENI, 2008.

Intitulé du master : Sécurité informatique .

Semestre : S1.

UE : UEM112.

Titre de la matière : Piratage éthique et défense des systèmes.

Crédit : 4.

Coefficient : 2.

Objectifs de la matière : Cette matière permet de donner les principes du piratage informatique et leur permettra de devenir un hacker éthique. Elle se concentre sur le code de conduite et l'éthique du système d'attaque. La pensée et l'évolution de l'hacker criminel sont également abordées. Les étudiants acquièrent également une compréhension et une formation de base sur les facteurs de compromission des systèmes informatiques afin de les protéger des criminels. Seul le piratage éthique est abordé, ce qui établit une distinction claire entre piratage illégal et piratage éthique.

Connaissances préalables recommandées :

Contenu de la matière :

Chapitre 1 : Introduction et éthique.

1.Piratage éthique.

2. Éthique.

3. Engagements et rapports.

Chapitre 2 : Reconnaissance.

1. OSINT.

2. Reconnaissance passive et active.

3. Outils courants de reconnaissance.

Chapitre 3 : Piratage et doxxing Google.

1. Piratage Google.

2. Introduction au doxing.

Chapitre 4 : Ingénierie sociale.

1. Tendances humaines.

2. Ingénierie sociale.

3. Boîte à outils d'ingénierie sociale.

Chapitre 5 : Analyse.

1. Processus d'analyse.

2. Balayage ping.

3. Analyses de ports.

4. Nmap.

Chapitre 6 : Exploitation.

1. Comprendre l'exploitation.

2. Dépassements de tampons.

3. Cadres d'exploitation.

Mode d’évaluation : Contrôle continu et examen.

Références bibliographiques :

1. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy 2nd Edition.
2. Penetration Testing: A Hands-On Introduction to Hacking.

Intitulé du master : Sécurité informatique .

Semestre : S1.

UE : UET1.

Titre de la matière : DevOps.

Crédit : 2.

Coefficient : 1.

Objectifs de la matière : À l'issue de cette matière, les étudiants seront capables de gérer des projets logiciels à l'aide des méthodologies DevOps et Agile, de mettre en œuvre des pipelines CI/CD, d'automatiser les processus avec les outils DevOps, d'appliquer l'infrastructure en tant que code (IaC) et la conteneurisation, et d'intégrer les meilleures pratiques de sécurité (DevSecOps) au cycle de développement.

Connaissances préalables recommandées : Principes de base du développement logiciel (programmation et contrôle des versions), fondamentaux des réseaux informatiques et de la cybersécurité et la familiarité avec les concepts du Cloud Computing.

Contenu de la matière :

1. Introduction à la gestion de projets logiciels en DevOps.
   - DevOps dans le contexte de l'ingénierie logicielle et de la sécurité des réseaux.
   - Différences entre la gestion de projet traditionnelle et Agile et DevOps.
   - Collaboration entre les équipes de développement, d'exploitation et de sécurité.
2. Méthodes de développement agiles en DevOps.
   - Frameworks Scrum et Kanban pour DevOps.
   - Outils agiles : Jira, Trello, projets GitHub.
   - Gestion du développement logiciel de manière itérative et incrémentale.
3. Contrôle de version et collaboration.
   - Git et GitHub/GitLab/Bitbucket pour le contrôle de version.
   - Meilleures pratiques : Stratégies de ramification, revues de code et demandes de fusion.
   - Gestion des workflows de développement collaboratifs.
4. Intégration et déploiement continus (Continuous Integration & Continuous Deployment : CI/CD).
   - Principes des pipelines CI/CD.
   - Mise en place de pipelines avec Jenkins, GitHub Actions, GitLab CI/CD.
   - Stratégies de tests et de déploiement automatisés.
5. Infrastructure as Code (IaC) et conteneurisation.
   - Principes IaC : gestion de l'infrastructure avec du code.
   - Outils : Terraform, Ansible, Puppet.
   - Conteneurisation et orchestration : Docker, Kubernetes.

6. DevOps basé sur le Cloud.
   - Plateformes Cloud : AWS, Azure, Google Cloud.

- Outils DevOps Cloud-native : AWS CodePipeline, Azure DevOps.
- Gestion de l'infrastructure et de la sécurité Cloud.

7. Surveillance, journalisation et optimisation des performances.
   - Outils d'observabilité : Prometheus, Grafana, ELK Stack.
   - Surveillance et audit de la sécurité dans DevOps.
   - Réponse aux incidents et dépannage.
8. DevSecOps : intégration de la sécurité dans DevOps.
   - Sécurité Shift-left : intégration de la sécurité dès le début du cycle de vie du développement logiciel.
   - Outils de test de sécurité automatisés : SonarQube, OWASP ZAP, Snyk.
   - Bonnes pratiques de conformité et de sécurité.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Justin Domingus et John Arundel, Cloud Native DevOps with Kubernetes, 2nd Edition, O'Reilly Media, Inc., 2022.
2. Mark S. Merkow, Practical Security for Agile and DevOps, Auerbach Publications, 2022.
3. Bradley Smith, DevOps for the Desperate: A Hands-On Survival Guide, No Starch Press, Inc., 2022.
4. M. Krief, Learning DevOps: A comprehensive guide to accelerating DevOps culture adoption with Terraform, Azure DevOps, Kubernetes, and Jenkins, Packt Publishing, 2022.
5. Stephen Chin, Melissa McKay, Ixchel Ruiz, Baruch Sadogursky, DevOps Tools for Java Developers: Best Practices from Source Code to Production Containers, O'Reilly Media, 2022.
6. John Knight, Nate Swenson, The DevOps Career Handbook: The ultimate guide to pursuing a successful career in DevOps, Packt Publishing, 2022.
7. Michelle Ribeiro, Learning DevSecOps: Integrating Continuous Security Across Your Organization, O'Reilly Media, 2024.

Intitulé du master : Sécurité informatique .

Semestre : S1.

UE : UED1.

Titre de la matière : Au choix.

Crédit : 1.

Coefficient : 1.

Objectifs de la matière : Cette matière permet aux étudiants d'acquérir une vision plus large de leur domaine d'études et favorise une meilleure compréhension des enjeux sociaux, économiques et éthiques liées à l'informatique, ainsi qu'une capacité à communiquer efficacement et à s'adapter à des situations diverses qui peuvent se présenter. En d'autres termes, elle permet :

- Une ouverture à d'autres disciplines en relation avec le quotidien, afin de comprendre l'importance de la collaboration dans un environnement pluridisciplinaire.
- L'élargissement des horizons, ce qui favorise la compréhension de la pensée humaine dans le temps et l'espace.
- Développement de compétences transversales : communication, vision holistique, analyse et synthèse, capacité d'adaptation, etc.

Connaissances préalables recommandées : /.

Contenu de la matière :

1- Introduction à la discipline concernée (matière choisie).
2- Présentation des concepts fondamentaux.
3- Applications croisées avec l'informatique
4- Études de cas.

Liste des matières proposées pour le choix (Une matière par semestre).	
Catégorie : ''Sciences et culture''.	**Catégorie : ''Technique''.**
- Informatique verte (Green IT). - Gouvernance et transformation digitale. - L'impact des technologies sur le travail et les relations sociales. - Les technologies émergentes dans les services publics. - Biologie des systèmes et modélisation informatique. - Philosophie des sciences et de la technique. - Systèmes d'information environnementaux. - Droit du Numérique et Protection des Données (RGPD). - Psychologie cognitive.	- Informatique fondamentale. - Génie logiciel. - Ingénierie des systèmes d'information. - Science des données. - Intelligence artificielle. - Sécurité informatique . - Réseaux et systèmes distribués. - Systèmes Cyber-Physiques. - Informatique visuelle. - Bio-informatique. - Calcul haute performance. - Informatique quantique.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques : L'enseignant propose des références selon la matière choisie.

Intitulé du master : Sécurité informatique .

Semestre : S2.

UE : UEF211.

Titre de la matière : Cryptographie et sécurité.

Crédit : 5.

Coefficient : 3.

Objectifs de la matière : Permettre aux étudiants d'approfondir leurs connaissances dans la sécurité informatique par l'étude de différentes techniques de chiffrement ainsi que leurs catégories et de l'initier à l'étude des crypto systèmes à partir de problèmes algébriques ou de problèmes de code correcteur d'erreurs. Il aura l'occasion aussi d'apprendre la gestion des clés.

Connaissances préalables recommandées : Notions pour la compréhension des corps, des codes linéaires ainsi que de leurs applications et des connaissances élémentaires apportées par la théorie des corps finis en outre des notions d'algèbre.

Contenu de la matière :

1. Introduction.

   Besoins de sécurité, courbes elliptiques, cryptosystèmes symétriques, cryptosystèmes asymétriques, fonctions de hachage, signature électronique, nouvelles tendances en cryptographie et cryptanalyse, …

2. Chiffrement.
   a. Chiffrement par blocs.
      - Les structures de Feistel.
      - DES. (Data Encryption Standard).
      - Faiblesses du D.E.S. et évolutions.
      - AES. (Advanced Encryption Standard).
      - Modes de chiffrement symétrique.

   b. Chiffrement de flux.
      - Les LFSR classiques.
      - Utilisation moderne des LFSR.
      - RC4.
      - Comparaisons des chiffrements par blocs et par flots.

   c. Chiffrement par clé publique.
      - Concept.
      - Merkle-Hellman.
      - RSA : Rivest - Shamir – Adleman.
      - El Gamal.
      - L'utilisation des courbes elliptiques.
      - Comparaisons.

3. Authentification.

a. Protocoles, principes.
b. Techniques d'authentification.
c. Signature par clés publiques.
d. Sécurité des fichiers.
e. Algorithmes, exemples.

4. La gestion des clés.
   a. Distribution des clés.
   b. Échange des clés.
   c. Diffie Hellman.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

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.
5. Takanori Isobe, Santanu Sarkar.Progress in Cryptology, Springer International Publishing, 2022.
6. W. Stallings. "Computer Security: Principles and Practice". Editions Prentice Hall. 2011.
7. Didier Müller. Les Codes secrets décryptés. City Editions, 2007.
8. Renaud Dumont : Cryptographie et Sécurité informatique. Université de Liège 2010.
9. Touradj Ebrahimi, Franck Leprévost, Bertrand Warusfel, Cryptographie et sécurité des systèmes et réseaux, Hermès - Lavoisier 2006.
10. M. T. Goodrich, R. Tamassia. "Introduction to Computer Security". Editions Pearson,International Edition. 2010.
11. W. Stallings. "Cryptography and Network Security: Principles and Practice". Editions Pearson,International Edition. 2010.
12. G. Avoine, P. Junod, P. Oechslin. "Sécurité Informatique". Editions Vuibert. 2010.

Intitulé du master : Sécurité informatique .

Semestre : S2.

UE : UEF212.

Titre de la matière : Sécurité criminalistique des bases de données.

Crédit : 4.

Coefficient : 3.

Objectifs de l'enseignement : Les organisations se concentrent désespérément sur l'innovation dans le monde actuel. Des produits plus intelligents, plus compacts et plus rapides que jamais sont conçus et les services sont rendus plus accessibles que jamais. Quel est le résultat final ? Les ordinateurs embarqués sont présents dans une large gamme d'appareils, des serveurs informatiques aux réfrigérateurs, en passant par les compteurs d'énergie et les stimulateurs cardiaques. La plupart de ces systèmes doivent stocker et extraire des données de bases de données. Les bases de données ont toujours joué un rôle dans les cyberenquêtes et continueront de le faire à l'avenir.

Connaissances préalables recommandées :

Contenu de la matière :

1. Sécurité et technologies de l'information.
2. Authentification.
3. Contrôle d'accès.
4. Interrogation de données chiffrées.
5. Protection des communications entre bases de données.
6. Audit de sécurité.
7. Tests de sécurité.
8. Réaction à un incident.
9. Analyse forensique.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Database Security, 1st edition. Alfred Basta.

Intitulé du master : Sécurité informatique .

Semestre : S2.

UE : UEF221.

Titre de la matière : Réseaux avancés et sécurité.

Crédit : 5.

Coefficient : 3.

Objectifs de l'enseignement : - Permettre une compréhension approfondie des réseaux informatiques, couvrant les couches application, transport et réseau, ainsi que les concepts avancés des réseaux locaux, étendus et définis par logiciel. - Fournir une intelligence approfondie de la sécurisation des réseaux, quels que soient leur type et leur architecture. Admettre une capacité à identifier les meilleures pratiques, outils et méthodologies pour l'analyse et l'évaluation de la sécurité des réseaux, ainsi que la conception et la mise en œuvre des réseaux sécurisés.

Connaissances préalables recommandées : Notions de base des réseaux informatiques.

Contenu de la matière :

a. Paradigmes de communication réseau.
   1. Client/Serveur.
   2. Peer to peer.
   3. Publication/Abonnement.

b. Couche application.
   1. Protocoles : HTTP, FTP, TFTP, SIP, SMTP, DNS, CoAP, MQTT.
   2. VoIP, RoIP, messagerie instantanée, modèle Publication/Abonnement.

c. Couche transport.
   1. Multiplexage et démultiplexage.
   2. Protocoles : TCP, UDP, RTP, SCTP.

d. Couche réseau.
   1. Présentation d'IPv4 et IPv6.
   2. Routage IP (statique et dynamique), RIP, EIGRP, OSPF, IS-IS, BGP.
   3. Routage multicast.
   4. Gestion de la coexistence et tunnellisation IPv4/IPv6.
   5. Protocoles : ICMPv6 et MIP (IP mobile).

e. Réseaux locaux (LAN).
   1. VLAN (VTP, DTP, routage inter-VLAN).
   2. Redondance dans les réseaux locaux (STP, Rapid STP, MSTP, EtherChannel, HSRP).
   3. MPLS, NAT, PAT.

f. Réseaux étendus (WAN).
   1. Protocoles : PPP, PPPoE.
   2. Réseaux privés virtuels (VPN).

g. Couche liaison de données.
   1. Protocoles : ARP, RARP, HDLC, CSMA/CD, LLDP.

2. Chapitre 8 : Réseaux définis par logiciel (SDN).
3. Concepts et architecture des SDN.
4. Protocole OPENFLOW.
5. Contrôleurs SDN.

h. Virtualisation des fonctions réseau (NFV).
1. Introduction et architecture NFV (VNF, NFVi, MANO).
2. Algorithmes VNF (Placement, Ordonnancement, Migration, Chaînage, Multidiffusion).
3. Réseaux étendus définis par logiciel (SD-WAN).
4. Concepts et architecture SD-WAN.
5. Comparaison : SD-WAN et MPLS.

i. Introduction à la sécurité des réseaux.
1. Exemples d'architectures réseau.
2. Menaces et attaques réseaux courants.
3. Surveillance et prévention.
4. Analyse des menaces (outils).
5. Normes de sécurité réseau.

j. Infrastructures de sécurité réseau.
1. Réseau local virtuel (VLAN).
2. Sécurité des accès (pare-feu, WAF, proxy, NAC).
3. Sécurité des serveurs.
4. Systèmes de détection et de prévention des intrusions (IDPS).
5. Zones démilitarisées (DMZ).
6. Réseaux privés virtuels (VPN).
7. Principes et méthodes de conception d'une architecture réseau sécurisée.

k. Politiques et approches de sécurité réseau.
1. Solution Zero Trust.
2. Solutions SIEM (Security Information and Event Management).
3. Solutions IDS/IPS (S. de détection des intrusions/S. de prévention des intrusions).
4. Sécurité des accès.
5. Gestion des vulnérabilités.
6 Audit et conformité. - Formation et sensibilisation.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach. Pearson Editions.
2. Bonaventure, O., Networking: Principles, Protocols, and Practice (3rd Edition, 2021).
3. Pujolle, G., Réseaux logiciels - Volume 1, Virtualisation, SDN, 5G et sécurité (2015).

4. Huawei Technologies Co., Ltd. (2023). SDN and NFV in Data Communications and Network Technologies, Springer.
5. Bradai, A., et al., Software-Defined Networking (SDN) and Network Function Virtualization (NFV) (2020). 7. Zeeshan Qaiser, Computer Networking, Toronto Academic Press, 2024.
6. Ali Sadiqui, Computer Network Security, Wiley-ISTE, ISBN: 978-1-786-30527-5, June 2020, 272 pages.
7. J. Migga Kizza, Guide to Computer Network Security, Springer International Publishing, 2024, 654 p.
8. Charlie Kaufman, Radia Perlman, Mike Speciner and Ray Perlner, Network Security: Private Communication in a Public World (Prentice Hall Series in Computer Networking and Distributed Systems) Edition: 3, Addison-Wesley Professional, 2022, 544 pages.
9. William Stallings, ''Network Security Essentials: Applications and Standards'', Pearson, 2016.
10. Razi Rais, Christina Morillo, Evan Gilman, Zero Trust Networks: Building Secure Systems in Untrusted Networks, 2nd Edition, Oreilly, 2024.

Intitulé du master : Sécurité informatique .

Semestre : S2.

UE : UEF 222.

Titre de la matière : Cybercriminalité.

Crédit : 4.

Coefficient : 3.

Objectifs de l'enseignement : Permettre aux étudiants de connaître l'ensemble des actes criminels commis via un système informatique ou Internet, de détecter les diverses activités illégales telles que la fraude, l'escroquerie, le vol de données, et le piratage.

Connaissances préalables recommandées : /

Contenu de la matière :

Chapitre 1 : Fondements de la cybercriminalité.

1. Définition de la cybercriminalité.
2. La cybercriminalité contemporaine.
3. Criminalité terrestre et cybercriminalité.
4. Cybercriminalité et criminalité en col blanc.

Chapitre 2 : Le système informatique comme cible.

1. Infractions liées à l'accès non autorisé dans le cyberespace.
2. Menaces émergentes : cibles et formes attendues.
3. Autres infractions liées au piratage informatique et aux virus informatiques.
4. Modification non autorisée de programmes ou de données informatiques.

Chapitre 3 : Défis pour la justice pénale.

1. Motifs et types de cybercriminels.
2. Défis pour la justice pénale et les forces de l'ordre.
3. Juridictions transnationales.
4. Identification et suivi des preuves.

Chapitre 4 : Confidentialité, sécurité et contrôle de la cybercriminalité.

1. Anonymat, confidentialité et sécurité dans le cyberespace.
2. Stratégies et lois pour la prévention de la cybercriminalité.
3. Lois et conventions internationales sur la cybercriminalité.
4. Lutte contre la cybercriminalité en Algérie.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Computer Forensics and Cyber Crime: An Introduction, Marjie Britz.
2. Cybercrime strategy, NORWICH: TSO.
3. Gordon, S.: Exploring spyware and adware risk assessment. Presentation to the Computers and Security Institute Conference, Phoenix, Arizona.

Intitulé du master : Sécurité informatique .

Semestre : S2.

UE : UEM21.

Titre de la matière : Forensiques multimédia et sécurité.

Crédit : 4.

Coefficient : 2.

Objectifs de l'enseignement : Cette matière analyse en profondeur les avancées dans le domaine émergent de la criminalistique et de la sécurité multimédia en abordant des problématiques complexes telles que le tatouage numérique pour la protection des droits d'auteur, les empreintes digitales numériques pour le suivi des transactions et l'identification des sources des caméras numériques.

Connaissances préalables recommandées :

Contenu de la matière :

1. Introduction.
2. Stéganographie multimédia.
3. Filigrane multimédia.
4. Format multimédia.
5. Caractéristiques du masquage d'informations.
6. Caractéristiques du filigrane.
7. Techniques de filigrane.
8. Détection de modifications significatives dans les séquences image/audio/vidéo.
9. Filigrane neuronal profond.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. A. Bovik, Handbook of Image & Video Processing, Academic Press.
2. I.J. Cox, M.L. Miller, and J.A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, Inc., San Francisco.

Intitulé du master : Sécurité informatique .

Semestre : S2.

UE : UEM22.

Titre de la matière : Sécurité de l'IoT.

Crédit : 5.

Coefficient : 2.

Objectifs de l'enseignement : La sécurité de l'Internet des objets (IoT) vise à protéger les appareils et les communications des systèmes IoT en installant des mesures de protection et en évitant les pratiques susceptibles de conduire à des intrusions et des attaques. Cependant, la sécurité n'a jamais été une priorité absolue lors du développement de l'IoT, et par conséquent, les fournisseurs ont développé des solutions IoT dépourvues de fonctionnalités de sécurité complètes.

Connaissances préalables recommandées :

Contenu de la matière :

1. Contexte et aperçu des applications de l'IoT.
2. Architecture et protocoles de l'IoT.
3. Problèmes de sécurité et de confidentialité dans l'IoT.
4. Protocoles de sécurité de la couche de perception.
5. Protocoles de sécurité de la couche réseau.
6. Protocoles de sécurité de la couche application.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Practical Internet of Things Security, Brian Russell and Drew Van Dure.
2. IoT Security and Privacy Paradigm, Pal Souvik, Díaz Vicente García, Le Dac-Nhuong.
3. IoT Security: Advances in Authentication, Madhusanka Liyanage.
4. The IoT Architect's Guide to Attainable Security & Privacy, David M. Wheeler.

Intitulé du master : Sécurité informatique .

Semestre : S2.

UE : UET2.

Titre de la matière : Gestion de projets informatiques.

Crédit : 2.

Coefficient : 1.

Objectifs de l'enseignement : Cette matière permet à l'étudiant :

- De comprendre les principes et les méthodes de gestion de projets informatiques.
- D'exécuter les différentes phases d'un projet informatique, de la conception à la clôture.
- D'acquérir les compétences en planification, organisation, suivi et contrôle de projets.
- D'identifier et gérer les risques liés aux projets informatiques.
- D'utiliser des outils et des techniques de gestion de projets informatiques.
- De travailler en équipe dans un contexte de gestion de projet.

Connaissances préalables recommandées : Génie logiciel et systèmes d'information.

Contenu de la matière :

1. Introduction à la gestion de projets informatiques.
   - Définition et enjeux de la gestion de projets informatiques.
   - Processus de production d'un projet informatique : processus de réalisation, processus de gestion, processus qualité.
   - Les différents types de projets informatiques (développement logiciel, infrastructure, etc.).
   - Les acteurs impliqués dans un projet informatique.
2. Méthodologies de gestion de projets.
   - Méthodologies traditionnelles (cycle en V).
   - Méthodologies agiles (Scrum, Kanban).
3. Planification et estimation.
   - Définition du périmètre et des objectifs du projet.
   - Découpage du projet en tâches (WBS).
   - Établissement du planning (diagramme de Gantt, PERT).
   - Estimation des ressources (temps, budget, personnel, coûts, COCOMO).
   - Utilisation d'outils de planification (Microsoft Project, Asana, etc.).
4. Gestion des risques.
   - Identification et analyse des risques (matrice SWOT, diagramme d'Ishikawa).
   - Évaluation de la probabilité et de l'impact des risques.
5. Suivi et contrôle.
   - Suivi de l'avancement du projet.
   - Gestion des changements.
   - Communication et reporting.
   - Tableaux de bord et de métriques clés de performance (KPI).
6. Gestion des ressources.
   - Identification des ressources nécessaires.
   - Allocation des ressources aux différentes tâches.
   - Gestion des conflits et des priorités.
7. Gestion de la qualité.

Définition des critères de qualité.
Mise en place de procédures de contrôle qualité.
Réalisation de tests et de validation.

8. Clôture du projet.
   - Documentation de la clôture du projet.
   - Transfert des connaissances et des compétences.
   - Évaluation de la satisfaction des parties prenantes.
   - Bilan du projet et identification des leçons apprises.
9. Outils de gestion de projets informatiques.
   - Logiciels de gestion de projets.
   - Systèmes de gestion de la connaissance.
   - Plateformes de communication et de collaboration.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Project Management Institute (PMI) 52021). A Guide to the Project Management Body of Knowledge (PMBOK Guide). https://www.pmi.org/.
2. Andrew Stellman, Jennifer Greene (2005). Applied Software Project Management. Series: Theory In Practice.
3. Kerzner, Harold 2017). Project Management: A Systems Approach to Planning, Scheduling, and Controlling. Wiley. https://www.wiley.com/.
4. S. Berkun (2008). Making Things Happen: Mastering Project Management (Theory I Practice). O'Reilly.
5. R. S. Pressman, B. R. Maxim (2014). Software Engineering: a Practionner's Approach. McGraww Hill.
6. McConnell, Steve (2006). Software Estimation: Demystifying the Black Art. Microsoft Press. https://www.microsoftpressstore.com/.
7. C. Aubry (2022). Scrum un outil convivial pour une agilité radicale. Editions Dunod.
8. Stephen H.Kan (2010). Metrics and Models in Software Quality Engineering (2nd Edition), Addison-Wesley Professional.
9. Linda Westfall (2009). The Certified Software Quality Engineer Handbook. Quality Press.
10. Murali Chemuturi (2010). Mastering Software Quality Assurance: Best Practices, Tools and Techniques for Software Developers. J. Ross Publishing.

Intitulé du master : Sécurité informatique .

Semestre : S2.

UE : UED2.

Titre de la matière : Au choix.

Crédit : 1.

Coefficient : 1.

Objectifs de la matière : Cette matière permet aux étudiants d'acquérir une vision plus large de leur domaine d'études et favorise une meilleure compréhension des enjeux sociaux, économiques et éthiques liées à l'informatique, ainsi qu'une capacité à communiquer efficacement et à s'adapter à des situations diverses qui peuvent se présenter. En d'autres termes, elle permet :

- Une ouverture à d'autres disciplines en relation avec le quotidien, afin de comprendre l'importance de la collaboration dans un environnement pluridisciplinaire.
- L'élargissement des horizons, ce qui favorise la compréhension de la pensée humaine dans le temps et l'espace.
- Développement de compétences transversales : communication, vision holistique, analyse et synthèse, capacité d'adaptation, etc.

Connaissances préalables recommandées : /.

Contenu de la matière :

1- Introduction à la discipline concernée (matière choisie).
2- Présentation des concepts fondamentaux.
3- Applications croisées avec l'informatique
4- Études de cas.

Liste des matières proposées pour le choix (Une matière par semestre).	
Catégorie : ''Sciences et culture''.	**Catégorie : ''Technique''.**
- Informatique verte (Green IT). - Gouvernance et transformation digitale. - L'impact des technologies sur le travail et les relations sociales. - Les technologies émergentes dans les services publics. - Biologie des systèmes et modélisation informatique. - Philosophie des sciences et de la technique. - Systèmes d'information environnementaux. - Droit du Numérique et Protection des Données (RGPD). - Psychologie cognitive.	- Informatique fondamentale. - Génie logiciel. - Ingénierie des systèmes d'information. - Science des données. - Intelligence artificielle. - Sécurité informatique . - Réseaux et systèmes distribués. - Systèmes Cyber-Physiques. - Informatique visuelle. - Bio-informatique. - Calcul haute performance. - Informatique quantique.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques : L'enseignant propose des références selon la matière choisie.

Intitulé du master : Sécurité informatique .

Semestre : S3.

UE : UEF311.

Titre de la matière : Sécurité des systèmes d'exploitation.

Crédit : 4.

Coefficient : 3.

Objectifs de l'enseignement : Permettre à l'étudiant de maîtriser la sécurité des systèmes d'exploitation : concepts fondamentaux, méthodes d'analyse et d'évaluation de la sécurité des systèmes d'exploitation (de bureau et mobiles). Se familiariser avec les problématiques liées à l'authentification, au contrôle d'accès et à l'intégrité des flux de contrôle.

Connaissances préalables recommandées : Notions de base des systèmes d'exploitation, des algorithmes, de la structure des machines et des mécanismes permettant la gestion des ressources de la machine, notamment le processeur et la mémoire et les bases de la sécurité informatique.

Contenu de la matière :

1. Informations générales sur la protection : Sécurité et système, informations générales sur la protection et concepts de sécurité logique.
2. Introduction à la sécurité des systèmes d'exploitation (Linux, Windows et Android).
3. Introduction à l'administration et au contrôle d'accès des systèmes d'exploitation (Linux, Windows et Android).
4. Mécanismes de sécurité et de protection.
   - Base de confiance UNIX.
   - Généralités UNIX.
   - Windows et son sous-système de sécurité.
   - Protection de la mémoire.
   - Authentification et identification, contrôle d'accès discrétionnaire aux objets, système d'autorisations.
   - Audit de sécurité.
5. Menaces et attaques contre les systèmes d'exploitation.
6. Principaux outils de sécurité.
   - Contrôle des autorisations.
   - Chiffrement et chiffrement des données.
   - Antivirus.

7 - Méthodes d'analyse et d'évaluation de la sécurité d'un système d'exploitation.

8 - Reprise après panne et méthodes de récupération.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Silberschatz. A., Galvin. P., Gagne. G., operating System Concepts, John Wiley & Sons, 2012.
2. Tanenbaum. A., systèmes d'Exploitation, Pearson, 2008.
3. Jaeger, Trent, Operating system security, Morgan & Claypool Publishers, 2008.

4. Andrew S. Tanenbaum, Herbert Bos, Modern Operating Systems, Pearson, 2023.
5. Cory Altheide, Harlan Carvey, Digital Forensics with Open-Source Tools, Syngress imprint of Elsevier.
6. Angus M.Marshall, “Digital forensics: Digital evidence in criminal investigation”, John Wiley and Sons.

Intitulé du master : Sécurité informatique .

Semestre : S3.

UE : UEF312.

Titre de la matière : Virtualisation, Cloud Computing et sécurité.

Crédit : 5.

Coefficient : 3.

Objectifs de l'enseignement : L'objectif de cette matière est de permettre à l'étudiant de se familiariser avec le Cloud Computing, en présentant les fondements de la virtualisation ainsi que les outils permettant de créer et de déployer des infrastructures Cloud et enfin les applications de la sécurité dans un tel environnement.

Connaissances préalables recommandées : Notions de virtualisation, de distributivité, de réseau, de Web, ...

Contenu de la matière :

1. Virtualisation.
   - Définitions de la virtualisation.
   - Machines virtuelles (virtualisation des postes de travail, virtualisation des serveurs).
   - Virtualisation des applications.
   - Virtualisation des données et du stockage.
   - Virtualisation des réseaux informatiques.
2. Définitions et historiques.
   - Définitions : Le Cloud et le Cloud Computing, le Cloud Computing d'un point de vue économique, et le Cloud Computing comme un espace virtuel.
   - Historique : Années 50, début des années 2000, ...
3. Modèles et services du Cloud Computing.
   - Modèles du Cloud.
   - Services Cloud : Infrastructure en tant que service (IaaS), Plateforme en tant que service (PaaS), et Logiciel en tant que service (SaaS).
   - Architecture des services cloud.
   - Autres services.
4. Architecture et typologie du Cloud Computing.
   - Architecture : N-Tiers, architecture orientée services (SOA), machine virtuelle, et virtualisation de fichiers.
   - Déploiement : Phase pilote, phase de déploiement et d'intégration, phase de pilotage du chargement.
   - Typologie : Cloud privé, Cloud public, Cloud communautaire, Cloud hybride, Cloud distribué, Inter-Cloud, et Multi-Cloud.
5. Exemples de Cloud.
   - DROPBOX, Plateforme Cloud Microsoft, Clouds commerciaux et principaux acteurs du marché.
   - Présentation d'OpenStack, OpenNebula.

- Exemples de Cloud pour le stockage.

6. Avantages et limites du Cloud.
   - Avantages du Cloud : Réduction des coûts, flexibilité et recentrage sur le cœur de métier.
   - Limites du Cloud : Maîtrise des pertes informatiques (confiées à un ou des tiers), problèmes de sécurisation des données informatiques.
7. Sécurité et confidentialité dans le Cloud.
   - Aspects généraux.
   - Problèmes de sécurité spécifiques.
   - Aspects contractuels.
   - Bonnes pratiques de sécurité.
   - Synthèse et aperçu. - Menace. - Types d'attaquants. - Risques de sécurité. - Conseils pour limiter les risques.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, “Cloud Computing: Principles and Paradigms”, John Wiley & Sons, 2010 (ISBN 9781118002209).
2. Lee Gillam, “Cloud computing”, Springer, 2010 (ISBN 9781849962414).
3. Zaigham Mahmood, Richard Hill, “Cloud Computing for Enterprise Architectures”, Springer, 2011 (ISBN 9781447122364).
4. Cigref Réseau des grandes entreprises, Fondamentaux du Cloud Computing – Le point de vue des grandes entreprises”, Mars 2013.
5. Romain Hennion, Hubert Tournier, Eric Bourgeois, Cloud Computing : Décider - Concevoir - Piloter - Améliorer, Eyrolles, 2012.
6. Guillaume Plouin, Cloud Computing, Sécurité, stratégie d'entreprise et panorama du marché, Collection InfoPro, Dunod, 2013.
7. Guillaume Plouin, Tout sur le Cloud Personnel, Travaillez, stockez, jouez et échangez... dans le nuage, Dunod, 2013.
8. Adora Nwodo, Confident Cloud: Uncover the Essentials of Cloud Computing (Confident Series, 17) Edition: 1, Kogan Page, 2024.
9. Naresh Kumar Sehgal, Pramod Chandra P. Bhatt, John M. Acken, Cloud Computing with Security and Scalability. Concepts and Practices Edition : 3, Springer, 2023.
10. Matthew Portnoy, Virtualization Essentials, Sybex, 2023.
11. Souvik Pal, Dac-Nhuong Le., Prasant Kumar Pattnaik : Cloud Computing Solutions: Architecture, Data Storage, Implementation, and Security, ISBN: 978-1-119-68202-8 May 2022.
12. Judith S. Hurwitz, Daniel Kirsch: Cloud Computing for Dummies, 2nd Edition, ISBN: 978-1-119-54671 July 2020.

Intitulé du master : Sécurité informatique .

Semestre : S3.

UE : UEF321.

Titre de la matière : Authentification et contrôle d'accès.

Crédit : 5.

Coefficient : 3.

Objectifs de l'enseignement : Cette matière permet aux étudiants d'avoir une idée sur les outils et les processus utilisés pour vérifier l'authentification, les modèles et méthodes de gestion des accès, et la description de la modélisation des mécanismes de contrôle d'accès.

Connaissances préalables recommandées : Notions de logique mathématique.

Contenu de la matière :

Chapitre 1 : L'authentification.

- Définition.
- Authentification et autorisation.
- Les méthodes d'authentification courantes.

Chapitre 2 : Généralités et politiques de la gestion des accès.

- Généralités à la gestion des accès.
- Les politiques discrétionnaires ou DAC.
- Les politiques obligatoires ou MAC.
- Les politiques basées sur la notion de tâche ou TBAC.
- Les politiques basées sur la notion de rôle ou RBAC.
- Les politiques basées sur la notion d'équipe ou TMAC.
- Les politiques basées sur la notion d'organisation ou ORBAC.

Chapitre 3 : La sécurité en entreprise.

- La notion de risque.
- La destruction des données.

Chapitre 4 : Les architectures de paiement électronique.

- Le SET.
- 3D-Secure.
- Autres solutions.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. William Stallings Lawrence Brown Computer Security: Principles and Practice Prentice Hall; Edition: 2 (9 Novembre 2011).
2. Renaud Dumont : Cryptographie et Sécurité informatique. Université de Liège 2010.
3. Peter Gutmann. Secure deletion of data from magnetic and solid-state memory 1996.
4. HUHNS, Michael N. Distributed Artificial Intelligence : Volume I. Elsevier, 2012.

Intitulé du master : Sécurité informatique .

Semestre : S3.

UE : UEF322.

Titre de la matière : Sécurité des applications Web et mobiles.

Crédit : 4.

Coefficient : 3.

Objectifs de l'enseignement : Comprendre les principes et concepts fondamentaux de la navigation Web sécurisée, l'architecture de développement Web, les principales vulnérabilités et attaques spécifiques sur le Web, ainsi que les mécanismes et les bonnes pratiques de développement et de configuration d'applications Web. Comprendre le rôle du chiffrement dans la sécurité des applications et appareils mobiles et décrire les scénarios courants d'application du chiffrement.

Connaissances préalables recommandées : Sécurité des réseaux et analyse des vulnérabilités numériques.

Contenu de la matière :

Chapitre 1 : Vulnérabilités et méthodes d'attaque.

- Différents types de hackers.
- Organisation et objectifs des équipes de hackers.
- Les phases d'intrusion.
- Analyse des vulnérabilités et vulnérabilités Zero-Day.
- Attaques par code malveillant.
- Attaques d'ingénierie sociale.
- Attaques d'applications.

Chapitre 2 : Modèle de sécurité Web.

- Le navigateur web comme système d'exploitation et plateforme d'exécution.
- Contrôle d'accès basé sur les permissions.
- Protocoles, isolation et communication.

Chapitre 3 : Sécurité des applications Web.

- OWASP - Top 10 des attaques.
- Techniques de protection des applications web.

Chapitre 4 : Objectifs et problèmes du HTTPS.

- Protocole SSL/TLS : rappel.
- Renforcer la sécurité grâce au HTTPS.
- Problèmes HTTPS : certificat falsifié, trafic mixte http/https, etc.

Chapitre 5 : Politique de sécurité du contenu (CSP : Content Security Policy).

- Web workers.
- Politiques de sécurité du contenu. - Isolation des trames (Sandboxed iFrames).

Chapitre 6 : Suivi de session et authentification.

- Comment authentifier un site web.

- Mécanisme sécurisé de surveillance de l'état entre client et serveur.
- Cookies et intégrité de session.

Chapitre 7 : Sécurité XML et services Web.

- Rappel sur les services Web.
- Sécurité en XML.
- Présentation de la technologie AJAX.
- Attaques contre AJAX et mécanismes de défense.

Chapitre 8 : Sécurité mobile.

- Technologies informatiques mobiles.
- Présentation de la sécurité informatique mobile.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Mavoungou S., Kaddoum G., Taha M., and Matar G., Survey on threats and attacks on mobile networks, https://ieeexplore.ieee.org/document/8272037.
2. Papageorgiou A., Strigkos M., Politou E., Alepis E., Solanas A., and Patsakis C., Security and privacy analysis of mobile health applications: the alarming state of practice, https://ieeexplore.ieee.org/document/8272037.
3. M. Oltrogge, E. Derr, C. Stransky, Y. Acar, S. Fahl, C. Rossow, G. Pellegrino, S. Bugiel, and M. Backes, “The rise of the citizen developer: Assessing the security impact of online app generators,” in 2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA, May 2018, pp. 634–647. [Online]. Available: https://doi.org/10.1109/SP.2018.00005.
4. M. Zalewski, The Tangled Web: A Guide to Securing Modern Web Applications, 1st ed. San Francisco, CA, USA: No Starch Press, 2011.

Intitulé du master : Sécurité informatique .

Semestre : S3.

UE : UEM321.

Titre de la matière : Criminalistique numérique.

Crédit : 4.

Coefficient : 2.

Objectifs de l'enseignement : Ce cours permet aux étudiants de comprendre le processus fondamental d'analyse des données collectées à partir d'appareils électroniques (ordinateurs, supports et autres preuves numériques). Ils se familiarisent avec les techniques et outils appropriés pour sécuriser, manipuler et préserver les preuves numériques et multimédias sur les scènes de crime.

Connaissances préalables recommandées : Systèmes informatiques, réseaux informatiques.

Contenu de la matière :

1. Introduction.
   - Gestion des incidents de sécurité des SI.
   - Problème de préservation des preuves.
   - Classification des incidents : Défaillances techniques versus catastrophes naturelles.
   - Évaluation des risques.
   - Objectif de l'analyse forensique.
   - Les différentes approches.
2. Forensique morte, forensique vivante.
3. Analyse mémoire.
   - Récupération des informations système.
   - Récupération des informations de processus.
   - Récupération des informations de fichiers/répertoires.
   - Récupération des informations des réseaux.
   - Récupération des informations de sécurité.
4. Récupération des informations sensibles.
   - Récupération des clés Wi-Fi.
   - Récupération des mots de passe des navigateurs.
   - Récupération des mots de passe des outils Microsoft.
   - Récupération des mots de passe des routeurs.
5. Extraction des clés AES contenues dans la RAM.
6. Outils logiciels (Autopsy, EnCase, etc.).

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Aitken, C.G.G., Stoney, D.A., The use of Statistics in Forensic Science, Ellis Horwood, Londres, 1991.
2. Ribaux, O., La recherche et la gestion des liens dans l'investigation criminelle : le cas particulier du cambriolage, thèse de doctorat, Institut de Police Scientifique et de Criminologie, Lausanne, 1997.

3. Robertson, B., Vignaux, G.A., Interpreting Evidence, John Wiley & Sons, Chichester, 1995.
4. Chuck Easttom, Digital Forensics, Investigation, and Response, ISSA, 2022.
5. Vashishth, Tarun, Cyber Forensics up and Running: A hands-on guide to digital forensics tools and technique, BPB Publications, 2023.
6. MUHIBULLAH. MOHAMMED, Windows Forensics Analyst Field Guide: Engage in proactive cyber defense using digital forensics techniques, Packt, 2023.

Intitulé du master : Sécurité informatique .

Semestre : S3.

UE : UEM322.

Titre de la matière : Programmation et sûreté des systèmes répartis.

Crédit : 5.

Coefficient : 2.

Objectifs de l'enseignement : Cette matière présente des bases de programmation parallèle et répartie à l'aide de langages de programmation déclaratifs et aussi des solutions aux problèmes de coût et de fiabilité des systèmes répartis.

Connaissances préalables recommandées : Notions système réparti.

Contenu de la matière :

Chapitre 1 : Agents et Systèmes Multi-Agents.

- Introduction.
- Motivations.
- Agent vs. Objet.
- Paradigme Multi-Agents.
- Modèles Multi-Agents.
- Le Standards de SMA : FIPA.

Chapitre 2 : Agents Mobiles/Code Mobile.

- Modèles d'exécution répartie : Échange de messages, Code référençable, Évaluation distante, Code à la demande.
- Infrastructure pour les agents mobiles : exécution, migration, communication, désignation et localisation, contrôle de l'utilisation des ressources, sécurité (PGP).

Chapitre 3 : Détection d'intrusion par les Agents mobiles.

- Introduction à la détection d'intrusions.
- Principes de détection - Approche comportementale - Approche par scénarios.
- Quelques outils de détection d'intrusions.
- Systèmes de détection d'intrusions (IDSs).
- Problèmes de fiabilité d'un système de détection d'intrusion.
- L'approche par agent mobile pour les IDS.
- Sécurité dans les Réseaux ad-hoc sans fils.

Chapitre 4 : Programmation Parallèle.

- Modèle PRAM.
- Le modèle BSP (Bulk Synchronous Parallel).
- Le parallélisme des tâches.
- Le parallélisme de données.
- Programmation fonctionnelle Bulk Synchronous Parallel ML(BSML).
- Programmation MPI.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Wooldridge M. An Introduction to MultiAgent Systems, John Wiley and sons, 2002.
2. FIPA: Foundation for Intelligent Physical Agents. Specifications. 1997. http://www.fipa.org.
3. Plate-forme JADE : Java Agent Development Framework, 2000. http://jade.tilab.com/.
4. Java Expert System Shell (JESS) http://herzberg.ca.sandia.gov/jess/.
5. AUML. The Agent Unified Modelling language, http://www.auml.org/.
6. Mobility: Aglets (www.trl.ibm.com/aglets/).
7. Joseph JaJa. An Introduction to Parallel Algorithms. Addison Wesley, 1992.
8. R. H. Bisseling. Parallel Scientific Computation. A structured approach using BSP and MPI. Oxford, University Press, 2004.

Intitulé du master : Sécurité informatique .

Semestre : S3.

UE : UET3.

Titre de la matière : Méthodologie de recherche.

Crédit : 2.

Coefficient : 1.

Objectifs de l'enseignement : Cette matière vise à enseigner aux étudiants les compétences et les connaissances nécessaires pour mener des recherches scientifiques efficaces. Il couvre les étapes clés de la recherche, de la formulation du sujet à la rédaction du rapport final, en passant par la revue de littérature, la conception de la recherche, la collecte et l'analyse des données, ainsi que la présentation orale des résultats.

Connaissances préalables recommandées : rédaction scientifique, langue utilisée.

Contenu de la matière :

1. Introduction à la recherche scientifique.
   - Définition et objectifs de la recherche scientifique.
   - Types de recherche (fondamentale, appliquée, etc.).
   - Rôle de la méthodologie dans la recherche.
   - L'importance de la maitrise de la langue utilisée.
   - Éthique de la recherche en informatique : plagiat, auto plagiat, IA générative (ChatGpt, Deepseek, etc.).
2. Formulation du sujet de recherche.
   - Identification et sélection d'un sujet de recherche pertinent.
   - Revue de littérature.
     - Recherche de sources d'information pertinentes (articles scientifiques, livres, etc.).
     - Analyse critique de la littérature existante (état de l'art).
     - Identification des lacunes dans l'état de l'art.
   - Définition de la problématique.
     - Formulation d'une question de recherche claire et précise.
     - Définition d'hypothèses de recherche.
   - Objectifs de la recherche.
     - Définition des objectifs spécifiques de la recherche cible.
     - Identification des résultats attendus.
3. Conception de la recherche.
   - Choix des méthodes de recherche appropriées (expérimentale, qualitative, quantitative, etc.).
   - Planification de la collecte des données (échantillonnage, outils de collecte, etc.).
   - Élaboration d'un plan de recherche.
4. Collecte des données.
   - Mise en œuvre du plan de recherche.
   - Utilisation des outils et techniques de collecte de données spécifiques à l'informatique.
   - Gestion et organisation des données collectées.
5. Analyse des données.
   - Utilisation de logiciels d'analyse de données.
   - Traitement et analyse des données collectées.

- Utilisation de méthodes statistiques ou d'autres techniques d'analyse appropriées.
- Interprétation des résultats et discussion des implications.

6. Rédaction du rapport de recherche.
   - Modes et structures de publication : article, brevet, thèse, livre, poster, communication orale…
   - Utilisation de logiciels de rédaction : LaTex, overleaf, etc.
   - Structure et organisation d'un rapport de recherche scientifique.
   - Rédaction claire et concise des différentes parties du rapport.
   - Présentation des résultats et discussion des conclusions.
   - Rédaction et styles des références bibliographiques (APA, IEEE, etc.) et des annexes.
7. Présentation orale des résultats.
   - Préparation et réalisation d'une présentation orale des résultats de recherche.
   - Maîtrise de la communication scientifique.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques :

1. Beaud, Michel (2020). L'art de la thèse. La découverte.
2. Stefan Kottwitz (2021). LaTeX Beginner's Guide: Create visually appealing texts, articles, and books for business and science using LaTeX. 2nd Edition, Packt Publishing.
3. Jean-Marie Dubois (2005). La rédaction scientifique : mémoires et thèses : formes régulières et par articles. Estem.
4. Michèle Lenoble-Pinson (1996). La rédaction scientifique : conception, rédaction, présentation. Signalétique, De Boeck Université.
5. Christine Gérard, Jean Germain (1985). Recherche bibliographique et documentaire : généralités. Faculté de philosophie et Lettres.

Intitulé du master : Sécurité informatique .

Semestre : S3.

UE : UED3.

Titre de la matière : Au choix.

Crédit : 1.

Coefficient : 1.

Objectifs de la matière : Cette matière permet aux étudiants d'acquérir une vision plus large de leur domaine d'études et favorise une meilleure compréhension des enjeux sociaux, économiques et éthiques liées à l'informatique, ainsi qu'une capacité à communiquer efficacement et à s'adapter à des situations diverses qui peuvent se présenter. En d'autres termes, elle permet :

- Une ouverture à d'autres disciplines en relation avec le quotidien, afin de comprendre l'importance de la collaboration dans un environnement pluridisciplinaire.
- L'élargissement des horizons, ce qui favorise la compréhension de la pensée humaine dans le temps et l'espace.
- Développement de compétences transversales : communication, vision holistique, analyse et synthèse, capacité d'adaptation, etc.

Connaissances préalables recommandées : /.

Contenu de la matière :

5- Introduction à la discipline concernée (matière choisie).
6- Présentation des concepts fondamentaux.
7- Applications croisées avec l'informatique
8- Études de cas.

Liste des matières proposées pour le choix (Une matière par semestre).	
Catégorie : ''Sciences et culture''.	**Catégorie : ''Technique''.**
- Informatique verte (Green IT). - Gouvernance et transformation digitale. - L'impact des technologies sur le travail et les relations sociales. - Les technologies émergentes dans les services publics. - Biologie des systèmes et modélisation informatique. - Philosophie des sciences et de la technique. - Systèmes d'information environnementaux. - Droit du Numérique et Protection des Données (RGPD). - Psychologie cognitive.	- Informatique fondamentale. - Génie logiciel. - Ingénierie des systèmes d'information. - Science des données. - Intelligence artificielle. - Sécurité informatique . - Réseaux et systèmes distribués. - Systèmes Cyber-Physiques. - Informatique visuelle. - Bio-informatique. - Calcul haute performance. - Informatique quantique.

Mode d'évaluation : Contrôle continu et examen.

Références bibliographiques : L'enseignant propose des références selon la matière choisie.