REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

OFFRE DE FORMATION MASTER

PROFESSIONNALISANT

Etablissement	Faculté / Institut	Département
USTO MB	FMI	Informatique

Domaine : Mathématique et Informatique

Filière : Informatique

Spécialité : Cybersécurité

Année universitaire : 2026 2027

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

عرض تكوين ماستر

مهني

المؤسسة	الكلية/ المعهد	القسم
جامعة العلوم والتكنولوجيا وهران محمد بوضياف	كلية الرياضيات وعلوم الحاسوب	علوم الحاسوب

الميدان : الرياضيات وعلوم الحاسوب

الشعبة : علوم الكمبيوتر

التخصص : الأمن السيبراني

السنة الجامعية: 2026 2027

SOMMAIRE

Lettre de Motivation

Oran, le 30 avril 2026

Objet : Demande d'habilitation d'une offre de formation Master Professionnalisant – Cybersécurité

Madame, Monsieur,

Nous avons l'honneur de soumettre à votre haute approbation le présent dossier de demande d'habilitation pour l'ouverture d'un Master Professionnalisant en « Cybersécurité », au sein du Département d'Informatique de la Faculté de Mathématiques et d'Informatique de l'Université des Sciences et de la Technologie d'Oran – Mohamed Boudiaf (USTO MB).

La cybersécurité constitue aujourd'hui l'un des enjeux stratégiques majeurs pour l'économie nationale et internationale. Face à la recrudescence des cybermenaces, à la numérisation croissante des services publics et privés, et aux exigences de conformité réglementaire (ISO 27001, RGPD), la demande en experts capables d'assurer la protection des systèmes d'information est en forte croissance.

L'équipe pédagogique, composée d'enseignants-chercheurs expérimentés du Département d'Informatique, a conçu ce programme en étroite concertation avec le monde socio-économique régional, notamment les entreprises Sonatrach et Oranovia, afin de répondre aux besoins concrets du marché du travail. Le programme assure une progression pédagogique cohérente des fondamentaux de la sécurité (S1) vers les pratiques professionnelles avancées (S3), et se conclut par un stage en entreprise (S4) sanctionné par un mémoire.

Nous restons à votre disposition pour tout complément d'information et vous prions d'agréer, Madame, Monsieur, l'expression de notre haute considération.

La Responsable de l'équipe de spécialité.

Sarâh BENZIANE, Maître de Conférence Classe A

I – Fiche d’identité du Master

Localisation de la formation :

ulté (ou Institut) : Mathématiques et Informatique
artement : Informatique

· Coordonnateurs :

esponsable de l'équipe du domaine de formation :

fesseur ou Maître de conférences Classe A) :
Nom & prénom : Benkamra Zohra
Grade : Maître de Conférences A
▯ : Fax : E - mail : zohra.benkamra@gmail.com

ه.بن قمرة زهرة
رئيسة ميدان الرياضيات
والإعلام الآلي

esponsable de l'équipe de la filière de formation :

tre de conférences Classe A ou B ou Maitre Assistant Classe A) :
Nom & prénom : NEGGAZ Nabil
Grade : Maître de Conférences A
▯ : 0550312000 Fax : E - mail : neggaz.nabil@gmail.com

esponsable de l'équipe de spécialité :

moins Maitre Assistant Classe A) :
Nom & prénom : Sarâh BENZIANE
Grade : Maître de CONFÉRENCE CLASSE A
▯ : 0770171858 Fax : E - mail : sarah_benziane1@yahoo.fr

Dr SARÂH BENZIANE
ENSEIGNANTE-CHERCHEURE

Partenaires de la formation *:

- autres établissements universitaires :

- entreprises et autres partenaires socio économiques :

atrach

zy

- Partenaires internationaux :

* = Présenter les conventions en annexe de la formation

4 – Contexte et objectifs de la formation

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

Filière Informatique :

Licence en Systèmes informatiques
Licence en Ingénierie des systèmes d'information et du logiciel

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

Le Master professionnel en cybersécurité vise à former des experts capables d'assurer la protection des systèmes d'information et des infrastructures critiques face aux cybermenaces croissantes. Les principaux objectifs incluent :

1. **Développer des compétences techniques avancées** : Maîtrise des technologies et des outils de cybersécurité tels que les pare-feu, les systèmes de détection d'intrusion, la cryptographie et la gestion des vulnérabilités.
2. **Comprendre les enjeux stratégiques de la cybersécurité** : Analyse des risques et conception de politiques de sécurité adaptées aux organisations.
3. **Acquérir une expertise en conformité réglementaire** : Connaissance des normes et des lois en matière de cybersécurité, telles que le RGPD ou les cadres ISO 27001.
4. **Maîtriser les techniques de réponse aux incidents** : Développement de capacités en gestion des crises cybernétiques, en analyse forensique et en récupération après incident.
5. **Promouvoir l'innovation et l'adaptation** : Savoir intégrer des solutions innovantes et anticiper les évolutions des menaces grâce à une veille technologique continue.
6. **Renforcer les compétences transversales** : Communication, gestion de projets, et collaboration au sein d'équipes pluridisciplinaires.

Connaissances acquises :

- ✓ Architecture des systèmes sécurisés.
- ✓ Cryptographie appliquée.
- ✓ Sécurité des réseaux et du cloud.
- ✓ Analyse des vulnérabilités et évaluation des risques.
- ✓ Méthodologies de tests d'intrusion (pentest).
- ✓ Concepts avancés de la cybersécurité, comme l'intelligence artificielle appliquée à la détection des menaces.

Ce programme prépare les diplômés à occuper des postes tels que consultant en cybersécurité, analyste SOC, responsable de la sécurité des systèmes d'information (RSSI), ou encore auditeur en sécurité.

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

Le Master professionnel en cybersécurité forme des experts capables de répondre aux besoins croissants des entreprises et organisations en matière de sécurité numérique. Les diplômés seront préparés à occuper des postes clés, grâce à des compétences techniques, stratégiques et réglementaires solides. Voici les profils et compétences métiers visés :

1. Consultant en Cybersécurité :

- ✓ Réaliser des audits de sécurité informatique et des tests d'intrusion.
- ✓ Élaborer des politiques de sécurité et des plans de continuité d'activité.
- ✓ Conseiller les entreprises sur les normes et la conformité réglementaire.

2. Analyste SOC (Security Operations Center):

- ✓ Surveiller en temps réel les incidents de sécurité.
- ✓ Analyser les logs et détecter les anomalies.
- ✓ Gérer les alertes et y répondre efficacement.

3. Responsable de la Sécurité des Systèmes d'Information (RSSI) :

- ✓ Définir et superviser la stratégie globale de cybersécurité del'organisation.
- ✓ Coordonner la gestion des risques et les plans de réponse aux incidents.
- ✓ Assurer la formation et la sensibilisation des équipes internes.

4. Ingénieur en Sécurité Réseaux et Systèmes :

- ✓ Concevoir, configurer et sécuriser les infrastructures réseau.
- ✓ Déployer et maintenir des outils de sécurité, tels que des pare-feu et systèmes de détection d'intrusion.
- ✓ Assurer la protection des données et la gestion des accès.

5. Analyste Forensique :

- ✓ Investiguer les incidents de sécurité et analyser les preuves numériques.
- ✓ Rédiger des rapports techniques pour appuyer les enquêtes.
- ✓ Collaborer avec les autorités judiciaires et les experts légaux.

6. Architecte Sécurité :

- ✓ Concevoir des infrastructures sécurisées adaptées aux besoins des organisations.
- ✓ Intégrer des solutions innovantes pour prévenir les cyberattaques.
- ✓ Réaliser des études d'impact et des plans d'amélioration continue.

Les compétences métiers visées permettent une insertion professionnelle rapide et promettent des opportunités dans divers secteurs, tels que les entreprises technologiques, les banques, les assurances, ou encore les administrations publiques.

D- Potentialités régionales et nationales d'employabilité des diplômés

Les diplômés du Master professionnel en cybersécurité bénéficient de nombreuses opportunités d'emploi, grâce à une demande croissante en experts en sécurité numérique à l'échelle régionale et nationale. Les potentialités d'employabilité se déclinent comme suit :

1. Régionales :

- ✓ **Secteur public** : Les administrations locales et régionales investissent dans la sécurisation de leurs systèmes d'information pour protéger les données des citoyens et assurer la continuité des services publics.
- ✓ **Entreprises industrielles** : Les grandes zones industrielles et technologiques régionales recherchent des spécialistes pour protéger leurs systèmes automatisés et infrastructures critiques.
- ✓ **PME et startups** : Les petites entreprises locales adoptent progressivement des solutions de cybersécurité pour répondre aux exigences de leurs partenaires et protéger leurs données.
- ✓ **Institutions financières** : Les banques et assurances régionales renforcent leurs équipes pour prévenir la fraude en ligne et sécuriser les transactions.

2. Nationales :

- ✓ **Infrastructures critiques** : Les secteurs de l'énergie, des télécommunications et des transports, qui sont stratégiques pour l'économie nationale, nécessitent des experts pour sécuriser leurs systèmes contre les cyberattaques.
- ✓ **Technologie et innovation** : Le développement des Smart Cities et des projets numériques nationaux offre des débouchés dans la conception et la mise en œuvre de solutions sécurisées.
- ✓ **Secteur bancaire et financier** : Les grandes banques nationales recrutent pour se conformer aux réglementations internationales (ex. : RGPD, ISO 27001) et protéger les actifs financiers.
- ✓ **Éducation et recherche** : Les universités et centres de recherche nationaux investissent dans des programmes de cybersécurité pour former davantage de spécialistes et développer des innovations dans le domaine.
- ✓ **Sécurité et défense** : Les agences nationales de sécurité et de défense ainsi que des données des citoyens recrutent pour faire face aux cybermenaces croissantes, notamment dans la cyberdéfense.

E – Passerelles vers d'autres spécialités

Aucune

F – Indicateurs de suivi de la formation

1. Satisfaction des Étudiants

- ✓ **Taux de satisfaction globale:** Mesure le degré de satisfaction des étudiants par rapport à la formation.
- ✓ **Perception de la pertinence des enseignements:** Évalue si les connaissances acquises sont utiles pour la profession.
- ✓ **Appréciation des méthodes pédagogiques:** Mesure l'efficacité des méthodes utilisées (cours magistraux, travaux pratiques, projets...).

2. Taux de Réussite

- ✓ **Taux de réussite aux examens:** Mesure la performance des étudiants.
- ✓ **Taux d'obtention du diplôme:** Indique l'efficacité du parcours de formation.

3. Insertion Professionnelle des Diplômés

- ✓ **Taux d'insertion professionnelle:** Mesure le pourcentage de diplômés ayant trouvé un emploi dans leur domaine.
- ✓ **Délai d'insertion:** Évalue le temps nécessaire pour trouver un emploi.
- ✓ **Salaire d'embauche:** Compare les salaires des diplômés avec ceux du marché.

4. Qualité des Enseignants

- ✓ **Qualifications des enseignants:** Vérifie si les enseignants possèdent les compétences requises.
- ✓ **Expérience professionnelle:** Évalue l'expérience des enseignants dans le domaine de la cybersécurité.
- ✓ **Participation à la recherche:** Encourage l'implication des enseignants dans des projets de recherche.

5. Adaptation aux Besoins du Marché

- ✓ **Collaboration avec les entreprises:** Mesure les liens entre la formation et le monde professionnel.
- ✓ **Mise à jour des programmes:** Évalue la fréquence de mise à jour des contenus pour s'adapter aux évolutions technologiques.

6. Ressources Pédagogiques

- ✓ **Qualité des équipements:** Évalue la disponibilité et la performance des équipements pédagogiques (laboratoires, logiciels...).
- ✓ **Accès aux ressources documentaires:** Mesure la richesse des bibliothèques et des bases de données.

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

15

Nom, prénom	Diplôme graduation + Spécialité	Diplôme Post graduation + Spécialité	Grade	Type d'intervention *	Emargement
Belbachir Khadidja	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Belmabrouk Karima	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Benziane Sarah	Ingéniorat en Informatique - option : Systèmes parallèles et distribués	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Dairi Abdelkader	Ingéniorat en Informatique - option : Systèmes d'information	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Dekhici Latifa	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Mouri Hayat	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Ougouti Souad	Ingéniorat en Informatique Option : Software	Doctorat en sciences - option : Informatique	MCB	Cours, TD, TP, Encadrement	
Meddeber Lila	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en électronique - option : Vision et Reconnaissance de Formes	MCA	Cours, TD, TP, Encadrement	
Kies Ali	SIR	SIR	MCA	Cours, TD, TP, Enc	

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

	+ Spécialité	+ Spécialité	Grade	d'intervention *	Emargement
Yedjour Dounia	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	Professeur	Cours, TD, TP, Encadrement	
Choucha Chems Eddine	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	MCB	Cours, TD, TP, Encadrement	
Neggaz Nabil	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Yedjour Hayat	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	Professeur	Cours, TD, TP, Encadrement	
Benkamra Zohra	Ingéniorat en MAthématique	Doctorate n Mathématique	MCA		
Belmabrouk Karima	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Benziane Sarah	Ingéniorat en Informatique - option : Systèmes parallèles et distribués	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	Dr SARAH BENZIANE ENSEIGNANTE CHERCHEURE
Boughara Asmaa	Ingéniorat en Informatique - option : Systèmes d'information	Doctorat en sciences - option : Informatique	MCB	Cours, TD, TP, Encadrement	
Dekhici Latifa	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	Professeur	Cours, TD, TP, Encadrement	
Guelta Bouchiba	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Ougouti Souad	Ingéniorat en Informatique Option : Software	Doctorat en sciences - option : Informatique	MCB	Cours, TD, TP, Encadrement	
Meddeber Lila	Ingéniorat en Informatique - option : Génie logiciel	Doctorat en électronique - option : Vision et Reconnaissance de Formes	MCA	Cours, TD, TP, Encadrement	
Khelifa Fatiha	Ingéniorat en Informatique - option :	Doctorat en sciences - option : Informatique	MCA	Cours, TD, TP, Encadrement	
Siham Oujdi	Ingéniorat en Informatique - option :	Doctorat en sciences - option : Informatique	MCB	Cours, TD, TP, Encadrement	

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

Etablissement de rattachement :

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

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)**

A- Laboratoires Pédagogiques et Équipements :

Salle de TP d'Informatique (Capacité : 20 postes) :

20 ordinateurs connectés à Internet, équipés des systèmes d'exploitation Linux/Windows, des outils de virtualisation (VirtualBox, VMware), et des logiciels spécialisés en sécurité : Kali Linux, Wireshark, Metasploit, Snort, Nessus, OpenVAS.

Salle de Lecture et Bibliothèque Spécialisée :

Accès aux ressources documentaires numériques et salle de travail personnel avec connexion haut débit.

B- Terrains de stage et formations en entreprise :

Les étudiants effectuent leur stage en entreprise au semestre 4 (130h) auprès de partenaires socio-économiques dans les secteurs suivants :

- Sonatrach – Direction Systèmes d'Information : sécurité des infrastructures industrielles et SCADA.

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

Chef du laboratoire N° Agrément du laboratoire
Date : 28/01/2025 Avis du chef de laboratoire : Avis favorable Mme Medjdoub Lila Université des Sciences et de la Technologie d'ORAN Mohamed BOUDIAF LABORATOIRE DE RECHERCHE DE SYSTÈMES INTELLIGENTS L.A.R.E.S.I.

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
Optimisation environnementale et économique des systèmes de production	C00L07UN310220230001	2023	2027

E- Espaces de travaux personnels et TIC :

Salle de Lecture, Bibliothèque, Salle des machines, Gsuites déjà acquis par l'université

II – Fiche d’organisation semestrielle des enseignements

(Prière de présenter les fiches des 4 semestres)

1- Semestre 1 :

Semestre	Unités d'Enseignement				Matière (s) constituant l'unité								
	Nature	Code	Crédits	Coeff.	Intitulés des matières	VHS	V.H Hebdomadaire				Crédits	Coeff.	Mode d'évaluation
						14 Sem	Cours	TD	TP	Autres			Examen / CC
S1	Unité d'Enseignement Fondamentale	UEF1	11	6	Designing and Managing Secure Systems	42h	1h30		1h30	1h	6	3	60% / 40%
					Ethical Hacking and Systems Defense	42h	1h30		1h30	1h	5	3	60% / 40%
		UEF2	9	6	Secured Systems Administration - Database Security	42h	1h30		1h30	6h	5	3	60% / 40%
					Cryptography	42h	1h30		1h30	1h	4	3	60% / 40%
	Unité d'Enseignement de Méthodologie	UEM1	6	4	Quantum Computing	42h	1h30	1h30		1h	3	2	60% / 40%
					Artificial Intelligence	42h	1h30		1h30	1h	3	2	60% / 40%
	Unité d'Enseignement Transversale	UET1	2	1	Research Methodology	42h	1h30		1h30	1h	2	1	60% / 40%
	Unité d'Enseignement de Découverte	UED1	2	1	Ethics and Computer Deontology	21h	1h30				2	1	100%
	Total du semestre 1		**30**	**18**		**294h**	**12h**	**1h30**	**9h**	**12h**	**30**	**18**	

2- Semestre 2 :

Semestre	Unités d'Enseignement				Matière (s) constituant l'unité									
	Nature	Code	Crédits	Coeff.	Intitulés des matières	VHS	V.H Hebdomadaire				Crédits	Coeff.	Mode d'évaluation	
						14 Sem	Cours	TD	TP	Autres			Examen	CC
S2	Unité d'Enseignement Fondamentale	UEF21	9	5	Data Security in Networks	63h	1h30	1h30	1h30	3h	5	3	60%	40%
					Vulnerability Analysis	63h	1h30	1h30	1h30	3h	4	2	60%	40%
		UEF22	9	5	Digital Forensics	63h	1h30	1h30	1h30	3h	5	3	60%	40%
					Advanced Cryptography	42h	1h30		1h30	1h30	4	2	60%	40%
	Unité d'Enseignement de Méthodologie	UEM21	6	4	Security in Mobile Environments	42h	1h30		1h30	1h30	3	2	60%	40%
					Web Application Security	42h	1h30		1h30	1h30	3	2	60%	40%
		UEM22	2	1	Information Coding and Compression	42h	1h30	1h30			2	1	60%	40%
	Unité d'Enseignement Transversale	UET21	2	2	Lean Startup	42h	1h30	1h30		1h30	2	2	60%	40%
	Unité d'Enseignement de Découverte	UED21	2	1	Augmented and Virtual Reality	21h	1h30				2	1	100%	
	Total du semestre 2		**30**	**18**		**420h00**	**13h30**	**7h30**	**9h00**	**15h00**	**30**	**18**		

3- Semestre 3 :

Semestre	Unités d'Enseignement					Matière (s) constituant l'unité								
S3	Nature	Code	Crédits	Coeff.	Intitulés des matières	VHS	V.H Hebdomadaire				Crédits	Coeff.	Mode d'évaluation	
						14 Sem	Cours	TD	TP	Autres			Examen	CC
	Unité d'Enseignement Fondamentale	UEF31	10	6	Multimedia Forensics And Security	42h	1h30		1h30	1h30	5	3	60%	40%
					Critical Infrastructure Security	63h	1h30	1h30	1h30	3h00	5	3	60%	40%
		UEF32	10	5	Secure Cloud Computing	63h	1h30	1h30	1h30	3h00	5	2	60%	40%
					Internet Of Things (Iot) Security	42h	1h30		1h30	1h30	5	3	60%	40%
	Unité d'Enseignement de Méthodologie	UEM31	6	4	Innovative Technologies and Security Economics	42h	1h30		1h30	1h30	3	2	60%	40%
					Machine Learning for Security	42h	1h30		1h30	1h30	3	2	60%	40%
	Unité d'Enseignement Transversale	UET31	2	1	Soft Skills & Professional Development	21h00	1h30				2	1	100%	
	Unité d'Enseignement de Découverte	UED31	2	2	Blockchain and Cryptocurrencies	21h00	1h30				2	2	100%	
	Total du semestre 3		**30**	**18**		**336h00**	**12h00**	**3h**	**9h**	**12h00**	**30**	**18**		

4- Semestre 4 :

Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Cybersécurité

Stage en entreprise sanctionné par un mémoire et une soutenance.

	VHS	Coeff	Crédits
Travail Personnel	130h	8	12
Stage en entreprise	130h	7	12
Séminaires	45h	3	6
Autre (préciser)			
Total Semestre 4	305h	18	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	270h	157.5h	67h30	67h30	562h30
TD	0	45h	0	0	22h30
TP	90h	15h	0	0	105h
Travail personnel					
Autre (préciser)					
Total	315h	187h30	67h30	67h30	600h
Crédits	60	20	6	6	**120**
% en crédits pour chaque UE	50%	6%	3%	3%	100%

III - Programme détaillé par matière

(1 fiche détaillée par matière)

Title of the Master: Cybersecurity

Semester: 01

Teaching Unit: Fundamental

Course: Designing and Managing Secure Systems (DMSS)

Course Objectives

- ✓ Equip students with the methodological frameworks to design secure systems from the ground up using **"Secure by Design"** paradigms.
- ✓ Master the **Saltzer and Schroeder design principles** as the foundational logic for building resilient system architectures.
- ✓ Shift focus from mere administration/configuration to the proactive engineering of secure environments.
- ✓ Develop expertise in threat modeling and risk mitigation integrated into the system lifecycle.

Course Content:

1. Foundations of "Secure by Design" Engineering

- Moving beyond perimeter security: The "Secure by Design" philosophy.
- The System Development Lifecycle (SDLC) vs. Secure SDLC.
- Introduction to foundational security properties: Confidentiality, Integrity, Availability (CIA) and Accountability.

2. The Saltzer and Schroeder Design Principles

- **Economy of Mechanism:** Keeping the design small and simple to reduce the attack surface.
- **Fail-Safe Defaults:** Ensuring access is denied by default unless explicitly granted.
- **Complete Mediation:** Every access to every object must be checked for authority.
- **Open Design:** Security should not rely on the ignorance of potential attackers (No "security by obscurity").
- **Separation of Privilege:** Requiring multiple conditions/keys to grant access to a restricted resource.
- **Least Privilege:** Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- **Least Common Mechanism:** Minimizing the amount of mechanism shared by more than one user and depended on by all users.
- **Psychological Acceptability:** Security mechanisms must be easy to use to ensure they aren't bypassed.

3. Advanced Secure Architectural Patterns

- Defense in Depth: Multi-layered security strategies.
- Zero Trust Architecture (ZTA): Principles of "never trust, always verify" applied to system design.
- Access Control Models (DAC, MAC, RBAC) through the lens of Complete Mediation.
- Secure communication protocols and data-at-rest protection.

4. Risk Assessment and Methodology-Driven Design

- **Threat Modeling:** Using frameworks like STRIDE or PASTA to identify flaws during the design phase.
- Identifying assets and mapping vulnerabilities to design choices.
- Implementation of risk mitigation techniques at the architectural level.

5. Systems Management and Resiliency

- Continuous auditing and monitoring as a design requirement, not an after-thought.
- Patching strategies and secure configuration management (Hardening).
- Designing for Incident Response: Building systems that are "Forensic-Ready".

6. Case Studies: From Design Failure to Secure Engineering

- Analyzing real-world breaches caused by violations of Saltzer and Schroeder principles (e.g., privilege escalation, unmediated access).
- Collaborative project: Designing a secure system prototype following a formal "Secure by Design" methodology.

Assessment Methods:

Assignments (40%): Case study analysis focusing on architectural flaws and a group project to design a system prototype with a formal security design document.

Examination (60%): Final exam evaluating theoretical understanding of design principles and their practical

application in complex scenarios.

Title of the Master: Cybersecurity

Semester: 01

Teaching Unit: Fundamental

Course: Ethical Hacking and Systems Defense (EHSD)

Course Objectives

- ✓ Develop a solid understanding of the principles and methodologies of ethical hacking.
- ✓ Equip students with the knowledge to identify, assess, and exploit system vulnerabilities.
- ✓ Provide practical skills for implementing robust defense mechanisms and mitigating security threats.
- ✓ Instill an understanding of ethical and legal boundaries in cybersecurity practices.

Recommended Prerequisite Knowledge

- ✓ Basic knowledge of operating systems, networking, and cybersecurity fundamentals.
- ✓ Familiarity with penetration testing tools and techniques is a plus but not mandatory.

Course Content

1. **Introduction to Ethical Hacking**
   Role of ethical hackers and scope of penetration testing.
   Legal and ethicalconsiderations.
2. **Phases of Ethical Hacking**
   Reconnaissance and information gathering.
   Scanning and enumeration of target systems.
   Gaining access, maintaining access, and covering tracks.
3. **Exploitation Techniques**
   Exploiting common vulnerabilities: web, network, and application.
   Tools and frameworks (e.g., Metasploit, Wireshark, Nessus, OpenVAS).
   Active Directory Attacks.
4. **System DefenseStrategies**
   Developing defense mechanisms using firewalls, IDS/IPS, EDR (Endpoint Detection and Response), SIEM integration and secure configurations.
   Threat hunting and proactive measures.
   Cloud Security Testing (AWS/Azure)
5. **Advanced Techniques and Methodologies**
   Wireless and mobile security.
   Social engineering attacks and countermeasures.
6. **Case Studies and LabActivities**
   Real-world ethical hacking scenarios and exercises. Hands-on labs to secure systems against identified threats.
7. **Professional Reporting and Remediation Tracking**

Assessment Methods

- ✓ **Lab Work:** Hands-on exercises covering ethical hacking tools and techniques, Individual project focused on assessing a system's security posture and implementing defenses (40%).
- ✓ **Examination**: Exam evaluating theoretical and practical understanding (60%).

References

✓ The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Engebretson, 2013,

✓ Certified Ethical Hacker (CEH) Version 11 Study Guide by Ric Messier, 2021.

✓ Hacking: The Art of Exploitation by Jon Erickson, 2010, 2nd Edition,
✓ OWASP Top 10 Vulnerabilities Guide,
✓ Penetration Testing Execution Standard (PTES),

Title of the Master: Cybersecurity

Semester: 1

UE Title: UEF2

Course:Secured Systems Administration - Databases Security (SSADS)

Course Objectives:

By the end of this course, students will be able to:

- ✓ Administer and secure operating systems and databases.
- ✓ Implement best practices for database security and data protection.
- ✓ Detect and mitigate database vulnerabilities and respond to security incidents.

RecommendedPrerequisites:

- Basic SQL queries (SELECT, INSERT, UPDATE, DELETE).
- Understanding of functional dependencies and normalization.
- Intermediate SQL (joins, subqueries, views).
- Transactions and concurrency control (ACID properties).
- User and privilege management in DBMS (GRANT, REVOKE).
- Backup and restore procedur

Course Content

Chapter I: Fundamentals and Hardening

- Securing the database instance (OS, file system).
- Managing access, roles (RBAC), and administrative privileges.
- Disabling risky features and services.
- Practical consolidation of SQL skills: transactions, views, and privilege management before applying hardening techniques.

Chapter II: Advanced Data Protection

- Data encryption: at rest (TDE) and in transit (SSL/TLS).
- Dynamic masking and anonymization of sensitive data.
- Securing stored procedures and triggers.
- Hands-on implementation of backup/recovery strategies aligned with encryption policies.

Chapter III: Threats and Offensive Defense

- In-depth analysis of SQL Injection (advanced techniques: time-based, error-based).
- Prevention mechanisms: prepared statements, input validation, Database Firewall (DBFW).
- Case studies of real-world breaches involving SQL injection and privilege escalation.

Chapter IV: Audit and Monitoring

- Native audit setup and log management.
- Intrusion detection and abnormal behavior analysis.
- Integration of open-source tools (pgAudit, MySQL Enterprise Audit) for compliance and forensic readiness.

Practical Work (Labs)

1. Security configuration audit on a standard DBMS (MySQL/PostgreSQL).
2. Simulation of SQL injection attacks and implementation of countermeasures.
3. Configuration of encryption for data flows and stored data.
4. Basic forensic analysis after a database compromise.
5. Transaction management and privilege auditing exercise to bridge theory and practice.

Assessment Methods

- Continuous assessment (labs, reports, participation): 40%.

- Final examination (theoretical + practical): 60%.
- Mini-project: securing a small database system with encryption, auditing, and privilege management.

References

- Lynch, C. F., & Walters, C. M. (2010). *Database Security: Principles and Practice.* Addison-Wesley.
- OWASP Database Security Project.
- Smith, J. D., & Jones, A. B. (2022). *Advanced Techniques for Detecting SQL Injection Attacks.* Journal of Computer Security, 30(2), 123-145.
- NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations.*
- Elmasri & Navathe, *Fundamentals of Database Systems* (for SQL consolidation).
- Bertino & Sandhu, *Database Security: Concepts, Approaches, and Challenges.*

Title of the Master: Cybersecurity

Semester: 1

UE Title: UEF2

Course Title: Cryptography

Course Objectives:

- ✓ Understand fundamental cryptographic concepts and their applications in securing systems.
- ✓ Differentiate between symmetric and asymmetric cryptography and their use cases.
- ✓ Implement cryptographic algorithms to secure communication and data storage.

Recommended Prerequisites:

Basic knowledge of algebra and number theory.

Course Content:

Chapter 1: Introduction to Cryptography

Historical evolution
Core concepts (confidentiality, integrity, authenticity, and non-repudiation).

Chapter 2: Symmetric Key Cryptography

Block ciphers (DES, AES), Stream
ciphers (RC4, Salsa20).

Chapter 3: Asymmetric Key Cryptography

Public/private keys, RSA, Diffie-Hellman, ECC.
Introduction to Post-Quantum Cryptography (PQC) standards (e.g., Kyber, Dilithium)
Key exchange vs. Digital signatures

Chapter 4: Hash Functions and Digital Signatures

MD5, SHA families, applications of digital signatures.
Secure Password Hashing: Salts, Peppering, and Argon2/bcrypt algorithms.
Digital signatures: Structure, trust, and validation.

Chapter 5: Applications of Cryptography

Securing communication (SSL/TLS), file and disk encryption.
Public Key Infrastructure (PKI): Certificate Authorities (CA) and Certificate management.
Enterprise Key Management: Hardware Security Modules (HSM) and Cloud KMS.
Introduction to Zero-Knowledge Proofs (ZKP) and Homomorphic Encryption.

Practical Work:

Implementing AES,
Simulating RSA/Diffie-Hellman key exchange
Exploring hashing techniques.

Assessment Methods:

- ✓ Continuous assessment: 40%.
- ✓ Final examination: 60%.

References:

- ✓ Buchmann, J. (2013). Introduction to Cryptography. Allemagne: Springer New York.
- ✓ Menezes, A. J., Katz, J., van Oorschot, P. C., Vanstone, S. A. (1996). Handbook of Applied

Cryptography. États-Unis: CRC Press.

✓ Delfs, H., Knebl, H., &Knebl, H. (2002). Introduction to cryptography (Vol. 2). Heidelberg: Springer.

✓ Aumasson, J. (2024). Serious Cryptography, 2nd Edition: A Practical Introduction to Modern Encryption. États-Unis: No Starch Press.

Title of the Master: Cybersecurity

Semester: 01

Teaching Unit: Methodological

Course: Quantum Computing (QC)

Course Objectives

- ✓ Introduce the fundamentals of quantum mechanics as applied to computing.
- ✓ Equip students with the knowledge of quantum algorithms and their applications.
- ✓ Develop an understanding of quantum computational models and their advantages over classical computation.
- ✓ Provide hands-on experience with quantum programming tools and frameworks.

Recommended Prerequisite Knowledge

- ✓ Strong foundation in linear algebra and complex numbers.
- ✓ Basic understanding of classical computer science concepts (e.g., algorithms, complexity).
- ✓ Familiarity with computational physics is beneficial but not mandatory.

Course Content

1. **Introduction to Quantum Computing**
   Quantum mechanicsprinciples: superposition, entanglement, and qubits.
   Differences between classical and quantum computing.
2. **Quantum Gates and Circuits**
   Single and multi-qubit gates (Pauli, Hadamard, CNOT).
   Representing quantum circuits with matrices and vectors.
3. **Quantum Algorithms**
   Quantum Fourier Transform and Grover's search algorithm.
   Shor's algorithm for factoring and its impact on cryptography.
4. **Quantum Error Correction**
   Principles of error detection and correction in quantum systems.
   Fault-tolerant quantum computing.
5. **Hands-On Quantum Programming**
   Introduction to quantum programming platforms (e.g., IBM Qiskit, Google Cirq). Designing and running quantum experiments.
6. **Applications and Challenges**
   Cryptographic applications and quantum-resistantalgorithms.
   Real-world use cases: optimization, machine learning, and drug discovery.

AssessmentMethods

- ✓ **Programming Assignments**: Exercises using quantum programming frameworks, Design and implementation of a quantum algorithm to solve a specific problem (40%).
- ✓ **Examinations**: Exam covering theoretical and practical aspects of quantum computing (60%).

References

- ✓ *Quantum Computation and Quantum Information* by Michael A. Nielsen and Isaac L. Chuang, 2010,
- ✓ *An Introduction to Quantum Computing* by Phillip Kaye, Raymond Laflamme, and Michele Mosca, 2007
- ✓ IBM Q Experience and Qiskit Tutorials,
- ✓ Quantum Algorithm Zoo by the National Institute of Standards and Technology (NIST),

- ✓ Lecture notes from MIT's OpenCourseWare on Quantum Computation.

Title of the Master: Cybersecurity

Semester: 01

Teaching Unit: Methodological

Course:**Artificial Intelligence (AI)**

Course Objectives

- ✓ Understand and apply supervised and unsupervised learning techniques.
- ✓ Evaluate machine learning models using appropriate metrics to ensure reliability and accuracy.
- ✓ Understand the intersection of AI and cybersecurity, including threat detection, intrusion prevention, and incident response.
- ✓ Develop AI-powered tools for anomaly detection, malware identification, and user behavior analysis.

Recommended Prerequisite Knowledge

- ✓ Familiarity with concepts like probability distributions, mean, variance, standard deviation, and hypothesis testing.
- ✓ Awareness of working with sequential data (e.g., stock prices or IoT sensor data).
- ✓ General awareness of what machine learning is and its applications.

Course Content

1. Introduction to Artificial Intelligence

What is AI?
History of AI
Applications of AI
Ethics and Challenges in AI

2. **Data Science Fundamentals for AI**

Introduction to Data Science Data
Collection and Cleaning
Exploratory Data Analysis (EDA)
Feature Engineering

3. Machine Learning

Overview of Machine Learning
Supervised Learning
Unsupervised Learning
Evaluation of Machine Learning Models

4. Computer Vision

Introduction to Computer Vision
Image Fundamentals
Image Processing
Feature Detection and Matching Deep
Learning for Computer Vision

5. Real applications of Artificial intelligence

AI-driven Threat Intelligence
Detection of Deepfakes and AI-Based Cyberattacks
Biometric Security and Facial Recognition Blockchain
and AI in Cybersecurity
Case Studies and Practical Projects

Assessment Methods

- ✓ **Assignments**: Regular assignments analyzing secure design case studies, group project to design a secure system prototype with proper documentation (40%).
- ✓ **Examination**: Exam focusing on theoretical understanding and application (60%).

References :

- ✓ The Data Science Handbook,Authors: "Carl Shan , William Chen , Henry Wang , Max Song",
- ✓ Deep Learning, authors:"IanGoodfellow and YoshuaBengio and Aaron Courville" (MIT Press 2016),
- ✓ Artificial Intelligence for Cybersecurity,Editors:"Mark Stamp, Corrado Aaron Visaggio, Francesco Mercaldo, Fabio Di Troia" (Springer Nature 2022)

Title of the Master: Cybersecurity

Semester: 01

Teaching Unit: Discovery

Course: Ethics and Computer Ethics (ECE)

Course Objectives

- ✓ Develop an understanding of ethical theories and their application in the field of computer science.
- ✓ Explore issues related to digital privacy, intellectual property, and professional responsibilities.
- ✓ Equip students with the knowledge to make informed decisions regarding ethical dilemmas in computing practices.
- ✓ Promote awareness of international standards, laws, and professional codes of conduct.

Recommended Prerequisite Knowledge

- ✓ Basic understanding of computing principles and technologies.
- ✓ Awareness of cybersecurity and data protection issues is beneficial.

Course Content

1. **Foundations of Ethics and Morality**
   Ethical theories: deontology, utilitarianism, and virtue ethics.
   Principles of moral reasoning and decision-making.
   Applying moral reasoning to cybersecurity crisis management.
2. **Ethics in Computing**
   Digital privacy and surveillance. Intellectual property rights and plagiarism.
   Cybersecurity ethics: responsibilities of professionals and users.
   Vulnerability Disclosure: Responsible vs. Full Disclosure.
3. **Professional Codes of Conduct**
   Analysis of standards from ACM, IEEE, (ISC)² Code of Ethics and other organizations. Case studies of ethical challenges in professional practice.
4. **Legal and RegulatoryFrameworks**
   International and national laws on data protection (e.g., GDPR).
   Policies on cybersecurity and responsible AI use.
5. **EmergingEthical Challenges**
   Ethics in artificial intelligence and machine learning.
   Social implications of digital technologies (e.g.,bias, misinformation).
   The ethics of paying ransoms in Ransomware attacks.
6. **Case Studies and Debates**
   Examination of real-world scenarios involving ethical dilemmas in technology.
   Interactive sessions to debate diverse perspectives on computingethics.

AssessmentMethods

- ✓ **Case Analysis and debates**: Write-ups analyzing ethical dilemmas and group debates on contemporary issues in computing ethics (40%).
- ✓ **Examination:** Exam focusing on ethical theories and applications (60%).

References

- ✓ *Computer Ethics* by Deborah G. Johnson and Keith W. Miller, 5th Edition, 2018.
- ✓ *Ethics for the Information Age* by Michael J. Quinn, 6th Edition, 2015,
- ✓ The Cambridge Handbook of Information and Computer Ethics by Luciano Floridi,
- ✓ ACM Code of Ethics and Professional Conduct,
- ✓ IEEE Code of Ethics.

Title of the Master: Cybersecurity

Semester: 01

Teaching Unit: Transversal

Course: Research Methodology (RM)

Course Objectives:

- ✓ Develop essential skills for conducting scientific research and writing.
- ✓ Understand research design, methodologies, and data analysis techniques.
- ✓ Learn to present and publish research findings effectively.

Recommended Prerequisites:

General understanding of academic writing.

Course Content:

1. **Introduction to Research:**
   Research types, ethics, and significance in cybersecurity.
   Research Design and Methods: Quantitative, qualitative, and mixed methods.
2. **Data Collection and Analysis:**
   Surveys, experiments, statisticaltools,
   Practical Work: Statistical software (SPSS, R).
3. **AcademicWriting:**
   Structuring papers, referencing, and avoiding plagiarism.
   Known Word and Latex Templates.
   Practical Work: Scientific writing tools, bibliographical writing tools
4. **PresentationSkills:**
   Creating research posters and delivering effective presentations.
   Using AI bots to enhance presentations content.

Practical Work: Presentations tools, AI bots

Assessment Methods

- ✓ Continuous assessment (assignments, research proposal, project): 40%.
- ✓Exam: 60%.

References:

- ✓ Rajasekar, D., & Verma, R. (2013). *Research methodology*. Archers & Elevators Publishing House.
- ✓ Gupta, A., & Gupta, N. (2022). *Research methodology*. SBPD publications.
- ✓ Poulain, N. (2020). LaTeX pour les enseignants. Royaume-Uni: EDITION MARKETING.

Title of the Master: Cybersecurity

Semester: 02

Teaching Unit: Fundamental

Course: Data Security in Networks (DSN)

Course Objectives

The course "Data Security in Networks" aims to equip students with a solid understanding of the key principles and practices for securing data in networked environments. First, a deep understanding of the fundamental principles of network security is given. Students will explore the major threats to computer networks, as well as the techniques and protocols used to protect data in transit. They will then learn about potential threats to data confidentiality, integrity, and availability, as well as the cryptographic techniques and protocols used to protect data during transmission and storage.

Recommended Prerequisites:

Network Course (L2 S4) of the SI/
ISI Bachelor's Degree – Data Knowledge.

Content:

Chapter 1: Review of Network Protocols

- OSI/TCPIP Model: layers and functionalities
- Network layer protocols: IPv4, IPv6, routing
- Transport layer protocols: TCP, UDP
- Application layer protocols: HTTP, FTP, DNS
- Review of analysis tools
- Deep Packet Inspection (DPI) and analysis of encrypted traffic (TLS SNI/JA3).

Chapter 2: Fundamental Principles of Network Security

- Security concepts: confidentiality, integrity, availability (CIA), securing network devices
- Common network threats and vulnerabilities to data security
- Mitigation techniques
- Types of attacks: interception, interruption, modification, fabrication
- Attacks on network protocols: spoofing, sniffing, DDoS
- Advanced Persistent Threats (APT) lateral movement in networks.

Chapter 3: Infrastructures for Network and Data Security

- Definition and importance of infrastructures for securing a network
- Role of infrastructures in threat prevention, detection, and response
- VLANs and VPNs (IPsec, SSL/TLS, WireGuard).
- Proxy servers and security gateways
- Firewalls (Stateful, NGFW, WAF).
- IDS/IPS (Intrusion Detection/Prevention Systems)
- Authentication servers and identity management
- Secure access solutions (Zero Trust, NAC)
- Securing Wireless Networks: WPA3, 802.11i
- Security in Internet of Things (IoT) Networks
- SASE (Secure Access Service Edge) and SD-WAN Security foundations.

Chapter 4: Data Security in Networks

- Overview of Data Security Concepts
- Data Management
- CIA Triad: Confidentiality, Integrity, and Availability
- Databasesecurity
- Securing Data in TCP/IP Networks

Legal, Ethical, and Regulatory Aspects of Data Security

Network-level Data Loss Prevention (DLP) and exfiltration detection via NetFlow.

Chapter 5: Data Security in Cloud and Virtualized Networks

Cloud Security Models and Shared Responsibility

Securing Data in Cloud Storage and Virtual Networks

Encryption in Cloud Services

Hybrid Networks and Data Security Challenges

Assessment Methods

✓ Continuous assessment :40%.

✓Exam: 60%.

Reférences

- ✓ Cisco Networking Academy, CCNA Security Course Booklet Version 1.1, 2 Ed., Cisco Press
- ✓ William Stallings, Lawrence Brown, Computer Security: Principles and Practice, Prentice Hall William Stallings
- ✓ Network Security Essentials: Applications and Standards, Prentice Hall [ISBN: 0-13- 610805-9] Chong Ed. Kim.
- ✓ Fundamentals of Network Security Firewalls & VPNs, Jones & Bartlett Publishers [ISBN: 0-76-379130-X] William (Chuck) Easttom.
- ✓ Computer Security Fundamentals, 2nd Edition Ed., Que Michael Goodrich, Roberto Tamassia, Introduction to Computer Security, Addison Wesley
- ✓ Michael Buckbee (2020). Data Security: Definition. Explanation and Guide. p1 - 12;.
- ✓ W3Schools. Database Security. p1-2.

Title of the Master: Cybersecurity

Semester: 02

Teaching Unit: Fundamental

Course: Vulnerability Analysis (VA)

Course Objectives

Equip students with the skills to identify and analyze security vulnerabilities in various systems and applications.

Provide knowledge of vulnerability assessment methodologies and tools.

Enable students to recommend and implement remediation strategies to mitigate identified vulnerabilities.

Recommended Prerequisite Knowledge

Basic knowledge of operating systems and networking concepts.

Familiarity with cybersecurity fundamentals, including common threats and vulnerabilities.

Course Content

1. **Introduction to Vulnerabilities**
   - Definition and types of vulnerabilities.
   - The vulnerability lifecycle and its impact on cybersecurity.
   - Vulnerability databases: NVD, MITRE CVE, and CISA KEV.
2. **VulnerabilityAssessmentMethodologies**
   - Frameworks and standards (e.g., OWASP, CVSS). Manual vs. automated vulnerability assessment.
   - Risk-Based Vulnerability Management (RBVM) vs. Compliance-based.
3. **Tools for VulnerabilityAssessment**
   - Overview of tools like Nessus, OpenVAS, and Qualys.
   - Network scanning and web application vulnerability analysis.
   - Software Composition Analysis (SCA) for open-source vulnerabilities.
4. **Vulnerability Management Process**
   - Vulnerability prioritization using CVSS scores.
   - Steps for effective remediation and patch management.
5. **Reporting and Documentation**
   - Creating effective vulnerability reports.
   - Communicating risks and mitigation steps to stakeholders.
   - Tracking remediation and SLA (Service Level Agreements).
6. **PracticalLabs and Case Studies**
   - Simulated vulnerability assessment and analysis scenarios.
   - Real-world case studies of notable vulnerabilities and breaches.

AssessmentMethods

- ✓ **Lab Work**: Hands-on exercises using vulnerability assessment tools, detailed vulnerability assessment and mitigation plan for a specific system (40%).
- ✓ **Examination**: Final exam evaluating theoretical and practical understanding (60%).

References

- ✓ *The Art of Software Security Assessment: Identifying and Preventing Software*

Vulnerabilities by Mark Dowd, John McDonald, and Justin Schuh, 2006,
- ✓ *Hacking Exposed: Network Security Secrets and Solutions* by Stuart McClure, Joel Scambray, and George Kurtz, 7th Edition, 2012.
- ✓ National Vulnerability Database (NVD),
- ✓ OWASP Top 10 Vulnerabilities Guide.

Title of the Master: Cybersecurity
Semester: 02
Teaching Unit: Fundamental
Course: Digital Forensics (DF)

Course Objectives:

- ✓ Equip students with skills to investigate cyber incidents and gather digital evidence.
- ✓ Develop expertise in forensic tools and techniques for incident response.
- ✓ Understand legal and ethical aspects of digital forensics.

Recommended Prerequisites:

- ✓ Basic knowledge of operating systems and networking principles.
- ✓ Cybersecurity concepts.

Course Content:

1. **Introduction to Digital Forensics:**
   Role
   Processes
   Legalframeworks.
   Cyber dependent crime, cyber enabled Crime…
2. **Evidence Handling:**
   Incidence response
   Collectingevidence
   Types of evidence(file data; Meta data….) Chain of custody and maintaining integrity.
3. **Forensic Process, tools and Techniques:**
   Triage
   Disk imaging,
   Memory forensics
   Log analysis.
   Analysing data and writing reports
4. **NetworkForensics:**
   cloud data
   Packetanalysis
   Intrusion detection,
   Tracingattackers.
5. **Case Studies and Practical Labs:**
   Simulating forensic investigations using tools like FTK and EnCase.

Evaluation Methods:

- ✓ Practical assignments and lab reports: 40%.
- ✓ Midterm and final examinations: 60%.

References:

- ✓ Kävrestad, J., Birath, M., Clarke, N. (2024). Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications. Allemagne: Springer International Publishing, Imprint: Springer.
- ✓ André Årnes; Digital Forensics. (2017). Royaume-Uni: Wiley.

Title of the Master: Cybersecurity
Semester: 02
Teaching Unit: Fundamental
Course: Advanced Cryptography (AC)
Recommended Prerequisites:

- ✓ Completion of "Cryptography" in Semester 1.

CourseObjectives

- ✓ This course builds on the foundational concepts covered in "Cryptography I," focusing on advanced cryptographic techniques, post-quantum cryptography, and innovative protocols.
- ✓ Redundancies with the introductory course are avoided to ensure depth and novelty.
- ✓ Explore advanced cryptographic techniques and their applications.
- ✓ Analyze the security of cryptographic algorithms and protocols.

Content

Chapter 1: Advanced Symmetric Cryptography

Modes of Operation: Galois/Counter Mode (GCM), XTS-AES
Performance and Security Trade-offs in Symmetric Algorithms

Chapter 2: Elliptic Curve Cryptography (ECC)

Mathematical Foundations of ECC
Applications of ECC: Digital Signatures and Key Exchange
Comparison with RSA and DSA

Chapter 3: Cryptanalysis

Introduction to Cryptanalysis Techniques
Differential and Linear Cryptanalysis
Side-Channel Attacks (Timing and Power Analysis)

Chapter 4: Post-Quantum Cryptography

The Need for Post-Quantum Cryptographic Algorithms
Lattice-Based Cryptography: Learning With Errors (LWE)
Hash-Based Cryptography: Merkle Trees and XMSS
Code-Based Cryptography: McEliece and Niederreiter Schemes
Challenges in Post-Quantum Cryptography

Chapter 5: Advanced Protocols

Zero-Knowledge Proofs and Their Applications
Secure Multi-Party Computation
Cryptographic Protocols for Decentralized Systems

Chapter 6: Practical Applications and Case Studies

Cryptography in Cloud Computing Environments
Cryptographic Mechanisms in IoT Security

PracticalWork:

- ✓ Implement ECC operations using programming languages (e.g., Python, Java).
- ✓ Simulatecryptanalysis techniques likedifferentialcryptanalysis.
- ✓ Explore and implement lattice-based cryptographic algorithms using libraries such as NTRU.
- ✓ Develop a prototype demonstrating zero-knowledge proofs.

✓ Perform comparative performance analysis between post-quantum algorithms and traditional cryptographic methods.

Evaluation Methods: Continuous assessment (assignments, research on cryptographic trends): 60%.

✓ Final examination (theoretical and practical): 40%.

References:

✓ Easttom, W. (2022). *Modern cryptography: applied mathematics for encryption and information security*. Springer Nature.

✓ Aumasson, J. P. (2024). *Serious cryptography: a practical introduction to modern encryption.* No Starch Press, Inc.

✓ Nath, A. (2018). Python Cryptography. (n.p.): Amazon Digital Services LLC - KDP Print US.

Title of the Master: Cybersecurity

Semester: 02

Teaching Unit: Methodological

Course: Web Application Security (WAS)

Course Objectives

- ✓ Provide students with a comprehensive understanding of common vulnerabilities and security risks in web applications.
- ✓ Teach secure coding practices to prevent and mitigate common web-based attacks.
- ✓ Familiarize students with tools and techniques for testing the security of web applications.

Recommended Prerequisite Knowledge

- ✓ Basic understanding of web development technologies (HTML, CSS, JavaScript).
- ✓ Knowledge of server-side programming (e.g., PHP, Python, or Java).
- ✓ Familiarity with network and cybersecurity fundamentals.

Course Content

1. **Introduction to Web Application Security**
   Overview of web application architectures.
   Common security challenges in web development.
   The HTTP Protocol from a security perspective
   (Headers, Cookies, Security Flags).
2. **Web Vulnerabilities and Exploitation**
   OWASP Top 10: Cross-Site Scripting (XSS), SQL Injection, CSRF, etc.
   ces points ont Déjà été vus
   Case studies of real-world web attacks.
3. **Authentication and Session Management**
   Secure implementation of authentication mechanisms.
   Modern Identity Protocols: OAuth 2.0, OpenID Connect, and
   JWT (JSON Web Tokens) security.
   Managing sessions securely and preventing session hijacking.
4. **Input Validation and Secure Coding**
   Principles of secure input validation and sanitization.
   Implementation of Content Security Policy (CSP) and Secure
   Headers (HSTS, X-Frame-Options).
   Preventing injection attacks and other user-input vulnerabilities.
5. **Tools for Web Security Testing**
   Overview of tools such as Burp Suite, OWASP ZAP, and Nikto.
   Manual vs. automated web application testing.
6. **Advanced Topics in Web Security**
   Secure APIs and microservices.
   Protecting against DoS/DDoS and advanced persistent threats (APTs).
7. **Best Practices for Secure Development**
   Secure software development lifecycle (SDLC) principles.
   Continuous integration and security testing.

Assessment Methods

- **Lab Work**: Hands-on testing and securing web applications using tools and scripts, develop or secure a sample web application, identifying and fixing vulnerabilities (40%).
- **Examination**: Exam assessing theoretical knowledge (60%).

References

- ✓ *Web Application Security, A Beginner's Guide* by Bryan Sullivan and Vincent Liu, 2011.
- ✓ *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws* by DafyddStuttard and Marcus Pinto, 2011,
- ✓ OWASP Top 10 Project,
- ✓ Web security tutorials on PortSwigger's Academy.

Title of the Master: Cybersecurity

Semester: 02

Teaching Unit: Methodological

Course: Security in Mobile Environments (SME)

Course Objectives: At the end of this module, students will be able to:

- ✓ Identify vulnerabilities specific to mobile devices.
- ✓ Assess the associatedrisks.
- ✓ Implement appropriate security measures to protect data and applications on mobile platforms.

Recommended Prerequisites:

A good understanding of mobile operating systems (Android, iOS), wireless networks (Wi-Fi, Bluetooth), and fundamental computer security principles (cryptography, vulnerabilities, attacks) is required to take this course.

Course Content:

1. **Introduction to Mobile Security:**
   History and challenges of mobile security.
   Mobile-specificthreatmodels.
   Common threats: Spyware (Pegasus-style),
   Smishing, and App-based malware.
   Common vulnerabilities (rooting, jailbreaking, phishing, etc.).
2. **Mobile Operating System Security:**
   Comparison of Android and iOS security models.
   Security mechanisms at the kernel and application levels.
   Privilege and permission management.
3. **Mobile Application Security:**
   Mobile application lifecycle from development to deployment.
   Common vulnerabilities in mobile applications (injection, cross-site scripting, etc.).
   Static and dynamic application security testing techniques.
4. **Mobile Network Security:**
   Mobile communication protocols (GSM, UMTS, LTE, 5G).
   Attacks on mobile networks (man-in-the-middle, interception, etc.).
5. **Data Protection on Mobile Devices:**
   Encryption of data at rest and in transit.
   Password management and authentication.
   Biometric authentication (Biometric API) and
   MFA (Multi-Factor Authentication)
   Data lossprevention.
6. **BYOD (Bring Your Own Device) Security:**
   Challenges and issues related to BYOD policies.
   Mobile Device Management (MDM) solutions.
7. **Current Trends in Mobile Security:**
   IoT and security.
   5G and its security implications.
   Artificial intelligence and mobile security.

AssessmentMethods:

- ✓ **ContinuousAssessment (40%):**Practicalassignments, quizzes, class participation.
- ✓ **Final Exam (60%):** Evaluation of theoretical and practical knowledge acquired throughout the semester.
- ✓ **References:**

Books:

- ✓ Antonatos, S., Ioannidis, S., &Keromytis, A. D. (2016). *Mobile Security: Principles and Practice*. Springer.
- ✓ Enck, W., Gilbert, P., Han, S., &Necula, G. C. (2014). *TaintDroid: Efficiently detecting security violations in Android applications*. In *Proceedings of the 2014 ACM SIGSAC conference on Computer and communications security* (pp. 839-852). ACM.

Research Articles:

- ✓ Consult scientific databases such as IEEE Xplore, ACM Digital Library, ScienceDirect for recent articles on specific mobile security topics.

Online Resources:

- ✓ OWASP Mobile Security Project: https://owasp.org/www-project-mobile-app-security/
- ✓ Android Security Documentation: https://source.android.com/docs/security
- ✓ iOS Security Guide: https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf [1]

Title of the Master: Cybersecurity

Semester: 02

Teaching Unit: Methodological

Course: Information Coding and Compression (ICC)

Course Objectives

The aim of this course is to familiarize students with data encoding and compression techniques such as channel encoding, source encoding, and image compression. The student will learn the basic principles for evaluating the advantages and disadvantages of various compression techniques, as well as the criteria for selecting a data compression technique.

Recommended Prerequisites:

Probability and statistics, information theory, signal processing.

Course Content:

Chapter 1: Fundamental Concepts of Source Coding and Channel Coding (2 Weeks)

Definition, difference, and importance of channel encoding and source encoding Source and source coding

Channel and channel coding Basic concepts of joint coding

Chapter 2: Entropy Codings (2 Weeks)

Review of information theory Entropy and measures of information

Huffman coding - Adaptive versions of Huffman and Shannon-Fano

Arithmetic coding

LZW coding

Evaluation criteria

Chapter 3: Channel Coding (4 Weeks)

Key concepts and definitions

General communication scheme and transmission channel Types of channels

Efficiency, redundancy, and channelcapacity

Channel coding and Shannon's second theorem. Channel coding strategies

Error-correcting codes (Hamming codes, linear codes, cyclic codes, Reed-Solomon codes, etc.) Turbo codes and LDPC codes

Performance of a coder

Application examples

Chapter 4: Lossy Compression Methods (3 Weeks)

General concepts and definitions

General scheme of transformation-based compression methods

Evaluation criteria (MSE, PSNR, CR, SSIM, etc.)

Description of the different parts (Transformation, Quantification, and EntropyCoding) Effects of transformation on the compression method

Effects of quantization and different types of quantization

Standards and organizations for image compression

Chapter 5: Image Compression Techniques (JPEG Case Study) (4 Weeks)

JPEG standard, principles, and history

DCT and its various versions. Properties and advantages 8x8

block division and 2D DCT

Quantization matrix
Zig-zag scanning
Entropycoding
MSE, PSNR, CR, SSIM calculations, and computational complexity
General overview of image compression methods based on DWT (Examples: EZW, SPIHT, JPEG2000), comparison with JPEG

AssessmentMethods:

- ✓ ContinuousAssessment: 40%
- ✓ Final Exam: 60%

References:

- ✓ M. Cover and J. A. Thomas, *"Elements of Information Theory"*, 2nd edition, Wiley Series in Telecommunications and Signal Processing, 2006.
- ✓ M. Barlaud, C. Labit, *"Compression and Coding of Images and Videos"*, Collection IC2, Ed. Hermes, 319p, 2002.
- ✓ K. Sayood, *"Introduction to Data Compression, Third Edition"*, Elsevier Inc., 2006.
- ✓ Olivier Rioul, *"Information Theory and Coding"*, Ed. Lavoisier, 2007.
- ✓ N. Moreau, *"Tools for Signal Compression: Applications to Audio Signals"*, Collection Télécom, Ed. Lavoisier, October 2009.
- ✓ J.C. Moreira, P.G. Farrell, *"Essentials of Error-Control Coding"*, John Wiley and Sons, Ltd, 2006.
- ✓ C. Berrou, *"Codes and Turbo Codes"*, Springer-Verlag France, 2007.

Title of the Master: Cybersecurity

Semester:02

Teaching Unit: Discovery

Course: Augmented and Virtual Reality (AVR)

Course Objectives: At the end of this module, students will be able to:

- ✓ Understand the fundamental principles of AR and VR technologies.
- ✓ Analyze the security and privacy challenges associated with AR/VR systems.
- ✓ Identify and evaluate potential threats and vulnerabilities in AR/VR environments.
- ✓ Explore and discuss security best practices and mitigation strategies for AR/VR applications.

Recommended Prerequisites: Basic understanding of computer graphics, 3D modeling, and networking concepts. Familiarity with cybersecurity fundamentals (threat modeling, risk assessment).

Course Content:

1. **Introduction to AR and VR:**
   Definitions, concepts, and key differences between AR and VR. Hardware components (head-mounted displays, sensors, input devices). Software development platforms and tools.
   Applications of AR and VR in various domains (gaming, healthcare, education, industry).

2. **Security Challenges in AR/VR:**
   Privacy concerns (data collection, user tracking, location privacy). Security risks (hacking, malware, data breaches, denial-of-service attacks). Social engineering and manipulation in VR environments.
   Physical safety and user well-being in immersive experiences.

3. **Vulnerabilities in AR/VR Systems:**
   Hardware vulnerabilities (sensors, displays, processing units).
   Software vulnerabilities (operating systems, applications, communication protocols).
   Network vulnerabilities (wireless communication, data transmission).
   Human factors and social engineering vulnerabilities.

4. **Security Best Practices and Mitigation Strategies:**
   Secure development practices for AR/VR applications.
   Data encryption and privacy-preserving techniques.
   Secure authentication and authorization mechanisms.
   Intrusion detection and prevention systems for AR/VR environments.
   User awareness and education regarding security risks.

5. **Emerging Trends and Future Directions:**
   5G and its impact on AR/VR security.
   Blockchain technology and its applications in AR/VR security.
   Ethical considerations and societal implications of AR/VR technologies.

Evaluation method

Exam:100%

Title of the Master: Cybersecurity
Semester: 02
Teaching Unit: Transversale
Course: Lean Startup

The world is currently experiencing an unprecedented acceleration in innovation and technological advancement, making the business environment increasingly complex and difficult to predict. In this context, the success of innovative projects no longer depends solely on the quality of an idea or the sophistication of a technology. Rather, it relies on entrepreneurs' ability to understand market needs, continuously test their assumptions, and rapidly adapt to changing conditions.

Against this backdrop, the **Lean Startup** module aims to introduce students to one of the most influential methodologies for creating and developing innovative ventures, developed by the American entrepreneur **Eric Ries**. This approach is based on continuous learning from the market through rapid experimentation, data-driven decision-making, and the efficient use of resources by minimizing waste.

The module also seeks to equip students, particularly those in scientific and technological disciplines, with the practical tools required to transform innovative ideas and research outcomes into viable and scalable business ventures.

1. Module Description

This module focuses on the study of concepts, methods, and tools associated with the Lean Startup methodology. It emphasizes the mechanisms for building innovative ventures in environments characterized by high levels of uncertainty through experimentation, rapid learning, and continuous validation of assumptions.

2. Learning Objectives

Upon successful completion of this module, students will be able to:

- Understand the fundamental principles and philosophy of the Lean Startup methodology.
- Transform an innovative idea or research outcome into a viable business project.
- Formulate and test the key assumptions underlying a venture.
- Design and develop a Minimum Viable Product (MVP).
- Analyze market data and make informed business decisions.
- Align innovation and scientific research with market needs and customer expectations.

3. Prerequisites

Students are expected to have prior knowledge in the following areas:

- Fundamentals of entrepreneurship.
- Basics of project management.
- Concepts of innovation and technological development.
- General research methodology.

4. Module Content

Unit 1: Introduction to Startups

- Definition and characteristics of a startup.
- Differences between traditional businesses and startups.
- Innovation and value creation.
- The nature of technology-based ventures in uncertain environments.

Unit 2: Lean Startup Methodology

- Origins and evolution of the Lean Startup approach.
- Core principles of the methodology.
- The Build–Measure–Learn feedback loop.
- The concept of Validated Learning.
- Resource optimization and waste reduction.

Unit 3: Customer Development

- Steve Blank's Customer Development methodology.
- Identifying real customer problems.
- Conducting customer interviews and analyzing findings.
- Building and testing value hypotheses.

Unit 4: Business Model

- Definition and importance of the business model.
- The Business Model Canvas framework.
- Customer segmentation.
- Developing a value proposition.
- Revenue streams and cost structure analysis.

Unit 5: Minimum Viable Product (MVP)

- Concept and definition of the Minimum Viable Product.
- The role of MVPs in reducing uncertainty and risk.
- Different types of MVPs.
- Applications of MVPs in digital, scientific, and technological projects.

Unit 6: Measurement and Analytics

- Key Performance Indicators (KPIs).
- Growth metrics and user behavior analysis.
- The AARRR framework (Acquisition, Activation, Retention, Referral, Revenue).
- Data-driven decision-making.

Unit 7: Strategic Adaptation and Decision-Making

- Understanding Pivot and Persevere decisions.
- Determining when to change strategic direction.
- Types of pivots in startup development.
- Analysis of successful international case studies.

Unit 8: Financing and Growth Strategies

- Early-stage funding sources.

- Angel investors and venture capital.
- Rapid growth strategies.
- Fundamentals of startup marketing and growth.

5. Practical Work

The practical component of the module is designed to enable students to apply the acquired knowledge through real-world projects and activities, including:

- Conducting interviews with potential customers.
- Designing a business model for an innovative venture.
- Developing a Minimum Viable Product (MVP).
- Analyzing data and making strategic business decisions.
- Delivering a startup pitch before an evaluation panel.

6. Assessment Methods

Assessment Component	Weight
Final Examination	40%
Group Project	40%
Tutorials and Practical Work	20%

7. Teaching and Learning Approaches

The module adopts modern educational approaches, including:

- Project-Based Learning (PBL).
- Experiential Learning.
- Multidisciplinary teamwork.
- Startup ecosystem simulation.
- Problem-solving-based learning.

8. Key References

- Eric Ries, *The Lean Startup*.
- Steve Blank & Bob Dorf, *The Startup Owner's Manual*.
- Alexander Osterwalder et al., *Value Proposition Design*.
- Alexander Osterwalder & Yves Pigneur, *Business Model Generation*.

9. Learning Outcomes

Upon successful completion of the module, students will be able to:

- Develop a testable and scalable startup project.
- Design an MVP that addresses market needs.
- Build a coherent and comprehensive business model.
- Apply validation and continuous learning methodologies.
- Demonstrate entrepreneurial thinking and decision-making skills in uncertain environments.

10. Relevance to Scientific and Technological Disciplines

This module serves as a bridge between academic knowledge and economic value creation. It contributes to:

- Transforming scientific research outputs into marketable products and services.
- Promoting a culture of innovation and scientific entrepreneurship.
- Supporting the creation of Deep Tech startups.
- Directing research efforts toward solving real economic and societal challenges.
- Strengthening the university's contribution to economic development and wealth creation.

Conclusion

The Lean Startup model represents one of the most significant methodological innovations in modern entrepreneurship. More than a set of management tools, it promotes a new mindset centered on continuous learning, rapid experimentation, and adaptability in the face of uncertainty.

From this perspective, a startup is viewed as a temporary organization searching for a repeatable and scalable business model rather than an entity executing a predefined business plan. Consequently, success depends on understanding customer needs, systematically validating assumptions, and making decisions based on evidence and real-world data.

Mastering this methodology enables students to enhance their innovation capabilities and transform ideas and research outcomes into ventures with significant economic and social impact, thereby contributing to the advancement of the knowledge economy and innovation-driven entrepreneurship.

Title of the Master: Cybersecurity

Semester: 03

Teaching Unit: Fundamental

Course: Multimedia Forensics And Security (MFS)

Course Objectives:

- ✓ Understand the principles and techniques of multimedia forensics.
- ✓ Analyze and investigate multimedia evidence (images, audio, video) for authenticity and integrity.
- ✓ Identify and extract relevant information from multimedia files.
- ✓ Apply forensic tools and techniques to investigate multimedia-related cybercrimes.
- ✓ Understand the legal and ethical considerations in handling and presenting multimedia evidence.

Recommended Prerequisites: Basic understanding of computer forensics principles. Familiarity with digital evidence handling procedures.

Course Content:

1. **Introduction to Multimedia Forensics:**
   Overview of multimedia forensics and its applications.
   Types of multimedia evidence (images, audio, video, 3D models). Challenges and limitations of multimedia forensics.

2. **Image Forensics:**
   Image acquisition and processing techniques.
   Image manipulation detection (copy-move, splicing, retouching).
   Exchangeable Image File Format (EXIF) data analysis.
   Steganography and steganalysis.

3. **Audio Forensics:**
   Audio recording and processing techniques.
   Audio editing and manipulation detection.
   Speaker identification and voice recognition.
   Audio watermarking and copyright protection.

4. **Video Forensics:**
   Video acquisition and processing techniques.
   Video manipulation detection (splicing, tampering, deepfakes). Video analysis for object recognition and tracking.
   Surveillance video analysis and interpretation.

5. **3D Model Forensics:**
   3D model acquisition and processing techniques. 3D model manipulation detection.
   3D model authentication and provenance.

6. **Forensic Tools and Techniques:**

Introduction to forensic software tools (e.g., Autopsy, The Sleuth Kit, open-source image analysis tools).
Digital evidence handling and preservation procedures.
Chain of custody and evidence documentation.

7. **Legal and Ethical Considerations:**
   Legal admissibility of multimedia evidence.
   Ethical considerations in handling and analyzing multimedia evidence.
   Privacy and data protection concerns.

Assessment Methods:

- ✓ **Continuous Assessment (40%):** Case studies, practical exercises using forensic tools, presentations.
- ✓ **Final Exam (60%)**

References:

Books:

- ✓ Stamm, M. C., &Kompanets, L. (2018). *Multimedia forensics*. CRC Press.
- ✓ Fridrich, J. (2009). *Digital image forensics*. Academic Press.

Research Articles:

- ✓ Consult scientific databases such as IEEE Xplore, ACM Digital Library, ScienceDirect for recent research articles on multimedia forensics.

Online Resources:

- ✓ Websites and resources from forensic software vendors.
- ✓ Online communities and forums dedicated to digital forensics and investigations.

Title of the Master: Cybersecurity

Semester: 03

Teaching Unit: Fundamental

Course: Critical Infrastructure Security (CIS)

Course Objectives:

- ✓ Understand the concept of critical infrastructure and its importance to national security.
- ✓ Identify and assess the vulnerabilities and threats facing critical infrastructure.
- ✓ Analyze the impact of cyberattacks on critical infrastructure operations.
- ✓ Develop and implement security measures to protect critical infrastructure from cyber threats.
- ✓ Understand the role of government, industry, and international cooperation in critical infrastructure protection.

Recommended Prerequisites: Basic understanding of cybersecurity concepts (threat modeling, risk assessment, incident response). Familiarity with networking and systems administration concepts.

Course Content:

1. **Introduction to Critical Infrastructure:**
   Definition and classification of critical infrastructure sectors (energy, transportation, healthcare, etc.).
   Interdependencies between critical infrastructure sectors.
   Importance of critical infrastructure protection to national security and economic stability.
2. **Threats and Vulnerabilities:**
   malwares "ICS-aware" (Stuxnet, Industroyer, ou Triton).
   Physical security threats (natural disasters, terrorism, sabotage).
   Human factors and operational risks.
   Emerging threats (IoT, AI, 5G).
3. **Impact of Cyberattacks on Critical Infrastructure:**
   Disruptions to service delivery and economic activity.
   Safety and security risks to human life and property.
   National security and geopolitical implications.
   Case studies of cyberattacks on critical infrastructure.
4. **Critical Infrastructure Protection Strategies:**
   Risk assessment and management methodologies.
   Network Segmentation: The Purdue Model and Industrial Firewalls
   Implementation of security controls (physical, technical, administrative).
   Incident response and recovery planning.
   Building cyber resilience in critical infrastructure systems.
5. **Government and Industry Roles:**
   Government regulations and policies related to critical infrastructure protection. Role of industry in implementing and maintaining cybersecurity measures.
   Public-private partnerships and information sharing.
   International cooperation and information exchange.

Assessment Methods:

- ✓ **Continuous Assessment (40%):** Case study analysis, research papers, presentations, class discussions.
- ✓ **Final Exam (60%)**

References:

Books:

- ✓ Shostack, A. (2014). *Threat modeling: Designing for security*. Addison-Wesley.
- ✓ Carr, R., & Weber, R. (2016). *Security architecture and design*. Addison-Wesley.

Government Reports:

- ✓ Reports from agencies like the Department of Homeland Security (DHS), the National Infrastructure Protection Center (NIPC).

Industry Standards:

- ✓ Critical Infrastructure Protection (CIP) standards from organizations like NERC (North American Electric Reliability Corporation).

Research Articles:

- ✓ Consult scientific databases such as IEEE Xplore, ACM Digital Library, ScienceDirect for recent research articles on critical infrastructure security.

Title of the Master : Cybersecurity Semester *:* 03

Teaching Unit: Fundamental

Course: Secure Cloud Computing (SCC)

Course Objectives:

- ✓ Understand the different cloud computing models (IaaS, PaaS, SaaS).
- ✓ Analyze the security risks and vulnerabilities associated with cloud environments.
- ✓ Evaluate and implement security controls for cloud-based systems.
- ✓ Understand the legal and regulatory compliance requirements for cloud computing.
- ✓ Explore emerging trends in cloud security (e.g., serverless computing, edge computing).

Recommended Prerequisites: Basic understanding of cloud computing concepts. Familiarity with cybersecurity principles (threat modeling, risk assessment, incident response).

Course Content:

1. **Introduction to Cloud Computing:**
   Cloud computing models (IaaS, PaaS, SaaS).
   Cloud deployment models (public, private, hybrid, multi-cloud). Benefits and challenges of cloud computing.

2. **Security Risks and Vulnerabilities in Cloud Environments:**
   Data breaches and data loss.
   Insider threats and abuse.
   Denial-of-service attacks.
   Malware and other malicious code.
   Misconfiguration and lack of visibility.

3. **Cloud Security Controls:**
   Access control and identity management.
   Data encryption and key management.
   Virtualization security.
   Network security (firewalls, VPNs, intrusion detection).
   Disaster recovery and business continuity.

4. **Compliance and Regulations:**
   Relevant regulations (e.g., GDPR, HIPAA, PCI DSS).
   Compliance audits and certifications (e.g., ISO 27001, SOC 2).
   Contractual agreements with cloud providers.

5. **Emerging Trends in Cloud Security:**
   Serverless computing security.
   Edge computing security.
   Security in containerized environments (Docker, Kubernetes).
   AI/ML for cloud security.

Assessment Methods:

- ✓ **Continuous Assessment (40%):** Case studies, research papers, presentations, class participation.
- ✓ **Final Exam (60%)**

References:

✓ Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ...&Zaharia, M. (2010). *Above the clouds: A Berkeley view of cloud computing*. [1] University of California, Berkeley, 4.

Title of the Master: Cybersecurity

Semester: 03

Teaching Unit: Fundamental

Course: Internet of Things (IoT) Security (IoTS)

Course Objectives

- ✓ Provide an understanding of IoT architectures and associated security risks.
- ✓ Equip students with the skills to secure IoT devices, networks, and systems.
- ✓ Explore threat modeling, risk mitigation strategies, and secure development practices for IoT.
- ✓ Understand legal, ethical, and privacy considerations in IoT deployments.

RecommendedPrerequisiteKnowledge

- ✓ Basic knowledge of networking protocols and wireless communication.
- ✓ Familiarity with cybersecurity concepts, including encryption and authentication.
- ✓ Awareness of embedded systems or hardware basics is beneficial.

Course Content

1. **Introduction to IoT Security**
   Overview of IoT architectures and ecosystems.
   Unique security challenges in IoT environments.
2. **ThreatLandscape in IoT**
   Common IoT vulnerabilities (e.g., insecure interfaces, poor device authentication).
   Threat actors and attack methods targeting IoT devices.
3. **Security Protocols and Mechanisms**
   Cryptographic methods for IoT: lightweight encryption algorithms.
   Secure communication protocols: MQTT, CoAP, and DTLS.
4. **Device Security and Hardening**
   Securingfirmware and updates.
   Device identity and authentication mechanisms.
5. **IoT Network Security**
   Segmentation and secure network design for IoT devices.
   Intrusion detection and prevention systems in IoT networks.
6. **IoTPrivacy and Ethics**
   Data protection regulations (e.g., GDPR).
   Ethical considerations for IoT security.
7. **Case Studies and Practical Applications**
   Analyzing real-world IoT security incidents.
   Hands-on labs: threat modeling and implementing security measures for IoT devices.

AssessmentMethods

- ✓ **Lab Work**: Hands-on activities focusing on IoT device and network security, securing an IoT system, including analysis and implementation of protections (40%).
- ✓ **Examination**: Exam covering theoretical and practical knowledge of IoT security (60%).

References

- ✓ *Practical Internet of Things Security* by Brian Russell and Drew Van Duren, 2nd Edition, 2018.
- ✓ *Internet of Things Security: Principles and Practice* by Fei Hu, 2016.
- ✓ Security and Privacy in Internet of Things (IoTs) Models, Algorithms, and Implementations by Fei Hu, 2016,
- ✓ OWASP IoT Project, https://owasp.org/www-project-internet-of-things/
- ✓ IoT Security Foundation Guidelines, https://iotsecurityfoundation.org/best-practice-guidelines/

- ✓ Tutorials and tools for IoT security (e.g., Shodan, https://www.shodan.io/dashboard).

Title of the Master: Cybersecurity Semester: 03
Teaching Unit: Methodological
Course: Innovative Technologies and Security Economics

Course Objectives:

- Explore emerging technologies shaping the future of cybersecurity beyond Blockchain (e.g., Confidential Computing, Zero-Trust Hardware).
- Introduce the **Security Economics** framework to evaluate security as an economic problem rather than just a technical one.
- Master **Attacker Economics** to understand the cost-benefit analysis from the threat actor's perspective.
- Equip students with the analytical tools (ROI, ALE, ROSI) to justify security budgets and strategic investments to corporate leadership.

Course Content:

1. Emerging Defensive Technologies

- **Beyond Blockchain:** Decentralized Identity (DID), Privacy-Preserving Computations, and Self-Sovereign Identity.
- **Confidential Computing:** Using Trusted Execution Environments (TEEs) and Enclaves to protect data in use.
- **AI-Driven Autonomous Defense:** Moving from Machine Learning detection to automated response and self-healing systems.
- **Post-Quantum Resilience:** Transitioning infrastructures to quantum-resistant standards.

2. Principles of Security Economics

- **The Market for Vulnerabilities:** Understanding the economics of Zero-Day exploits and bug bounty platforms.
- **Information Asymmetry:** Why security is a "Market for Lemons" and how it impacts product quality.
- **Externalities in Cybersecurity:** How the lack of security in one system affects the entire ecosystem (e.g., Botnets and IoT).

3. Attacker Economics (The "Business" of Cybercrime)

- **Cost of Attack vs. Potential Gain:** Modeling the attacker's effort, resources, and risk.
- **Economic Disruption:** Strategies to "raise the cost" for the attacker to make an intrusion financially unviable.
- **The Cybercrime Underground Economy:** Structure of Ransomware-as-a-Service (RaaS) and the specialization of labor in the dark web.

4. Business Value and Budget Justification

- **Quantitative Risk Analysis:** Moving from "High/Medium/Low" to financial impact models.
- **Key Metrics for Executive Boards:**
  - **ALE (Annual Loss Expectancy):** Calculating the expected cost of security failures.
  - **ROSI (Return on Security Investment):** Demonstrating the value of preventative measures.
- **Cost-Benefit Analysis:** Aligning security spending with organizational risk appetite and business goals.

5. Strategic Decision Making

- **Cyber Insurance:** The role of insurance in risk transfer and its economic impact on security standards.
- **Compliance vs. Security:** Evaluating the economic cost of non-compliance (GDPR, ISO 27001) versus the cost of implementation.

Assessment Methods:

Case Study (40%): Develop a "Security Business Case" for a corporate board, including threat modeling (Attacker Economics) and a financial justification (ROSI) for an innovative technology implementation.
Final Examination (60%)

Recommended References:

Security Economics: A Guide for Digitization by Tyler Moore.
Economics of Information Security and Privacy by Bruce Schneier and Ross Anderson.
Relevant NIST and ENISA reports on emerging technology trends and cyber risk quantification.

Title of the Master: Cybersecurity Semester :03

Teaching Unit: Methodological

Course: Machine Learning for Security (MLS)

Course Objectives:

- ✓ Understand the fundamentals of machine learning and its applications in cybersecurity.
- ✓ Apply machine learning algorithms for threat detection and classification (e.g., intrusion detection, malware analysis).
- ✓ Develop and evaluate machine learning models for security use cases.
- ✓ Understand the ethical and societal implications of using machine learning in cybersecurity.
- ✓ Explore emerging trends in machine learning for security (e.g., adversarial machine learning, explainable AI).

Recommended Prerequisites:

- ✓ Basic understanding of machine learning concepts (supervised, unsupervised, deep learning).
- ✓ Familiarity with programming languages (e.g., Python) and data analysis tools.
- ✓ Basic understanding of cybersecurity concepts (threats, vulnerabilities, network traffic analysis).

Course Content:

1. **Introduction to Machine Learning for Security:**
   Fundamentals of machine learning (supervised, unsupervised, reinforcement learning).
   Common machine learning algorithms for security (e.g., decision trees, support vector machines, neural networks).
   Data preparation and feature engineering for security data.
2. **Intrusion Detection Systems (IDS) with Machine Learning:**
   Anomaly detection and misuse detection techniques.
   Network traffic analysis and feature extraction.
   Developing and evaluating IDS models using machine learning.
3. **Malware Analysis and Classification:**
   Malware detection and classification techniques.
   Static and dynamic malware analysis.
   Feature extraction from malware samples (e.g., opcode sequences, API calls).
4. **Phishing Detection and Spam Filtering:**
   Techniques for detecting phishing emails and spam messages. Natural
   Language Processing (NLP) for text classification.
   Building and evaluating phishing detection models.
5. **Anomaly Detection in Security Logs:**
   Analyzing security logs for unusual patterns and anomalies.
   Developing anomaly detection models using unsupervised learning techniques. Alerting and response mechanisms for security log anomalies.
6. **Ethical and Societal Implications:**
   Bias and fairness in machine learning models.
   Privacy concerns and data protection.
   Explainability and transparency of machine learning models.
   The impact of machine learning on cybersecurity jobs and the workforce.
7. **Emerging Trends:**

Adversarial machine learning (attacks and defenses).
Explainable AI (XAI) for security.
Reinforcement learning for security automation.

Assessment Methods:

- ✓ **Continuous Assessment (40%):**
  Practical assignments (e.g., developing and evaluating machine learning models). Case studies and project proposals.
  Participation in class discussions and debates.
- ✓ **Final Exam (60%)**

References:

Books:

✓ Provost, F., & Fawcett, T. (2013). *Data science for business: What you need to know about data mining and predictive analytics*. O'Reilly Media.

✓ Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press.

Research Articles:

✓ Consult scientific databases such as IEEE Xplore, ACM Digital Library, ScienceDirect for recent research articles on machine learning for security.

Online Resources:

- ✓ Machine learning libraries and frameworks (e.g., scikit-learn, TensorFlow, PyTorch).
- ✓ Cybersecurity datasets and resources (e.g., UCI Machine Learning Repository, Kaggle).

Title of the Master: Cybersecurity Semester :03

Teaching Unit: Fundamental

Course: Blockchain and Cryptocurrencies (BC)

Course Objectives

- ✓ Provide an in-depth understanding of blockchain technology and its foundational principles.
- ✓ Explore cryptocurrency mechanisms, applications, and ecosystem dynamics.
- ✓ Equip students with the skills to evaluate, deploy, and develop blockchain-based solutions.
- ✓ Address the security and ethical considerations related to blockchain and cryptocurrency use.

RecommendedPrerequisiteKnowledge

- ✓ Basic understanding of computer networks and distributed systems.
- ✓ Familiarity with cryptographic principles such as encryption and digital signatures.
- ✓ Foundational knowledge of economics or financial systems is helpful but not mandatory.

Course Content

1. **Introduction to Blockchain**
   Core principles: decentralization, immutability, and transparency.
   Blockchain structures: blocks, chains, and consensus mechanisms (PoW, PoS).
2. **Cryptocurrency Fundamentals**
   Introduction to Bitcoin: architecture, mining, and transactions.
   Ethereum and smart contracts: programmable blockchain features.
3. **Advanced Blockchain Concepts**
   Layer 2 solutions and scalability challenges.
   Decentralized finance (DeFi) and non-fungible tokens (NFTs).
   Cross-chain communication and interoperability.
4. **Security in Blockchain and Cryptocurrencies**
   Common vulnerabilities in smart contracts and blockchains. Attacks on blockchain networks (e.g., 51% attacks, Sybil attacks). Wallet security and key management.
5. **Regulations and EthicalConsiderations**
   Global regulatory landscapes and challenges.
   Legal issues around cryptocurrencies and blockchain technologies.
6. **Blockchain Use Cases and Applications**
   Beyond cryptocurrencies: supply chain, healthcare, and identity management.
   Case studies of successful blockchain implementations.
7. **PracticalLabs and Project Work**
   Hands-on setup of blockchain nodes and exploration of public blockchains. Development and deployment of smart contracts using tools like Solidity and Truffle.

Assessment Methods

- ✓ **Examinations**: Exam testing theoretical and practical understanding (100%).

References

- ✓ The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT) by Antony Lewis, 2021.
- ✓ Mastering Blockchain, Second Edition, Imran Bashir, 2018,
- ✓ *Blockchain Basics: A Non-Technical Introduction in 25 Steps* by Daniel Drescher, 2017,
- ✓ Blockchain Technology Overview, NISTIR 8202, https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf

Title of the Master: Cybersecurity

Semester:03

Teaching Unit: Transversal

Course: Soft Skills & Professional Development

Course Objectives

This course aims to equip future cybersecurity experts with the behavioral and interpersonal competencies required to thrive in high-pressure environments.

- Enhance Emotional Intelligence: Develop self-awareness and empathy to manage high-stress situations (e.g., incident response).
- Master Technical Communication: Learn to translate complex security threats into understandable language for C-level executives and non-technical stakeholders.
- Strengthen Critical Thinking: Improve problem-solving frameworks and decision-making under pressure.
- Foster Ethical Leadership: Understand professional ethics, compliance, and the responsibility of handling sensitive data.
- Develop Career Readiness: Prepare for the global job market through personal branding and interview preparation.

Recommended Prerequisite Knowledge

- Understanding of fundamental concepts of interpersonal communication.

Course Content

1. Introduction to Soft Skills & Emotional Intelligence (EQ)
   - The difference between Hard Skills and Soft Skills.
   - Understanding EQ: Self-regulation, motivation, and empathy.
   - The importance of EQ in cybersecurity (managing burnout and high-pressure ops).
2. Communication skills
   - Understanding the communication loop, barriers (jargon, noise), and feedback mechanisms.
   - Verbal & Non-Verbal: tone, body language..
   - Active Listening
   - Public Speaking
   - Written Communication
3. Advanced Communication for Security Professionals
   - Crisis Communication: How to communicate effectively during a data breach or security incident.
   - Audience Adaptation: "Translating" technical jargon for management, legal, and HR teams.
   - Persuasion and negotiation: Getting buy-in for security budgets and policies.
4. Critical Thinking & Problem Solving
   - Analytical thinking techniques (Root Cause Analysis, SWOT).
   - Cognitive biases in security analysis and how to avoid them.
   - Decision-making frameworks for rapid incident response.
5. Teamwork, Collaboration & Conflict Resolution
   - Working in a Security Operations Center (SOC): Coordination and role management.
   - Managing conflict in cross-functional teams (e.g., DevSecOps).
   - Giving and receiving constructive feedback.
6. Professional Ethics & Responsibility
   - The ethics of hacking: White Hat vs. Grey/Black Hat boundaries.
   - Legal implications, compliance (GDPR/ISO), and professional integrity.
   - Social engineering awareness: The psychology of manipulation.
7. Time Management & Stress Resilience
   - Prioritization techniques (Eisenhower Matrix) for handling alert fatigue.

- Stress management strategies for cybersecurity professionals.
- Building resilience and maintaining work-life balance.

8. Career Development (World Skills Standard)

- Personal branding and professional networking (LinkedIn).

Assessment Methods

- Case Studies: Group analysis of a "Crisis Simulation" (how the team communicated and solved a breach).
- Presentations: Pitching a security solution to a "Board of Directors" (role-play).
- Worshops and serious games.
- Written exam assessing theoretical understanding of ethics, conflict resolution theories, and situational judgement tests.

References

- Goleman, D. (1995). *Emotional Intelligence: Why It Can Matter More Than IQ*.
- Carnegie, D. *How to Win Friends and Influence People in the Digital Age.*
- Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking* (for the psychology/comm aspect).
- Project Management Institute (PMI) Soft Skills Standards.
- ✓ WorldSkills Standards Specifications (WSSS) for Cyber Security (Skill 54).

VII - Avis et Visas des organes Administratifs et Consultatifs

Intitulé du Master: Cybersecurity

Comité Scientifique de département
Avis et visa du Comité Scientifique : Date : 10/03/2025
Conseil Scientifique de la Faculté (ou de l'institut)
Avis et visa du Conseil Scientifique : Date : 16/03/2025 د.محاج ايمان رئيسة المجلس العلمي لكلية الرياضيات والإعلام الآلي
Doyen de la faculté (ou Directeur d'institut)
Avis et visa du Doyen ou du Directeur : Date : 16/03/2025 الأستاذ جبار يحيى عميد كلية الرياضيات و الإعلام الآلي
Recteur de l'université
Avis et visa du Recteur de l'université : Date : أ.د حمو أحمد مدير جامعة وهران للعلوم والتكنولوجيا

VII - Avis et Visas des organes Administratifs et Consultatifs

Intitulé du Master: Cybersecurity

Comité Scientifique de département
Avis et visa du Comité Scientifique : Date :

Conseil Scientifique de la Faculté (ou de l'institut)
Avis et visa du Conseil Scientifique : Date : 19/03/2026

Doyen de la faculté (ou Directeur d'institut)
Avis et visa du Doyen ou du Directeur : Favorable Date : 24/03/2026

Recteur de l'université
Avis et visa du Recteur de l'université : Date :

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

سوناطراك

sonatrach

Société Nationale pour la Recherche, la Production
le Transport, la Transformation
et la Commercialisation des Hydrocarbures

Université des Sciences et de
la Technologie d'Oran
« Mohamed Boudiaf » USTO-MB

CONVENTION CADRE DE COOPERATION

DANS LES DOMAINES DE LA RECHERCHE SCIENTIFIQUE ET DU DEVELOPPEMENT TECHNOLOGIQUE

ENTRE

SONATRACH - DIRECTION CENTRALE RECHERCHE ET DEVELOPPEMENT (DC-R&D)

ET

L'UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE D'ORAN « MOHAMED BOUDIAF » USTO-MB

Entre,

La Société Nationale pour la Recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures, SONATRACH S.P.A, dont le siège social est sis à Djenane El Malik, Hydra, Alger, ci-après désignée dans tout ce qui suit par le terme : « SONATRACH » représentée par **Monsieur Mustapha Mohamed BENAMARA**, en sa qualité de Directeur Central Recherche et Développement, ayant tous les pouvoirs à l'effet de la présente Convention Cadre,

D'une part,

ET

L'université des Sciences et de la Technologie d'Oran « Mohamed BOUDIAF » USTO M-B, dont le siège social est sis à El M'naouar BP 1505, Bir El Djir 31000 Oran-Algérie, ci-après désignée dans tout ce qui suit par le terme : USTO M-B, représentée par Monsieur le Professeur **Ahmed Hamou**, en sa qualité Recteur de l'Université, ayant tous les pouvoirs à l'effet de la présente Convention Cadre,

D'autre part.

SOMMAIRE

PREAMBULE :

Considérant que :

- La SONATRACH, acteur majeur de l'industrie pétrolière, est une société en constante mutation technologique, dotée d'une direction chargée des activités de recherche et développement et dispose d'une expertise, d'un savoir-faire et des moyens qui peuvent contribuer à l'évolution de la coopération entre les deux Parties en matière de recherche scientifique et du développement technologique.

- L'USTO-MB est un établissement de formation et de recherche pluridisciplinaire, placé sous la tutelle du Ministère de l'Enseignement Supérieur et de la Recherche Scientifique.

- Les discussions menées entre les Parties à l'effet d'identifier des opportunités de coopération dans les domaines de la recherche et du développement technologique, dans le but de développer des techniques et des technologies innovantes.

- La volonté des Parties de conclure une convention (ci-après dénommée « Convention Cadre ») pour définir le cadre régissant la mise en œuvre de cette coopération.

- La présente Convention Cadre sera exécutée conformément, aux meilleures normes et exigences requises en matière de recherches scientifique, d'éthique et d'environnement.

- La recherche conjointe bénéficiera, autant que les moyens des Parties le permettent, d'une approche spécifique relative au secteur pétrolier et gazier en utilisant les ressources des deux parties dans le respect des normes algériennes, notamment les normes environnementales.

- Les Parties considèrent le développement des connaissances qui se traduira à travers par la mise au point des inventions, des procédures et procèdes, des papiers de recherche communs et des brevets, comme des éléments clés pour le développement de cette coopération.

Le présent préambule fait partie intégrante de la présente Convention Cadre.

Ceci exposé, les Parties conviennent de ce qui suit :

ARTICLE 01 : DEFINITIONS

Au sens de la présente Convention Cadre, les termes et expressions ci-après, s'entendent comme suit :

1.1. « Partie » : signifie, au sens de la présente Convention-Cadre, SONATRACH/DC R&D ou l'USTO-MB, désignés collectivement « les Parties » ;

1.2 « Contrat spécifique » signifie tout accord conclu entre les Parties en exécution de la présente Convention Cadre ;

1.3 « Développement Technologique » : est une phase de la recherche et développement (R&D) correspondant à la mise au point d'une invention, d'un procédé, d'un composé chimique ou d'un produit dans le domaine du Oil & Gas ;

1.4 « Recherche Scientifique » : l'ensemble des actions entreprises en vue de produire et de développer les connaissances scientifiques dans les domaines de l'énergie et du Oil & Gas et les autres axes de coopération intéressants les parties comme cités dans l'article 04.

Les termes au singulier s'entendent également au pluriel et réciproquement.

ARTICLE 02 : OBJET

La présente Convention Cadre a pour objet d'arrêter les principaux domaines de coopération, ses objectifs et de définir les conditions et modalités de mise en œuvre de la coopération en matière de Recherche Scientifique et du Développement Technologique.

La présente Convention Cadre constitue le cadre contractuel de référence pour toutes les actions d'intérêt commun qui viendraient à être initiées entre les Parties.

ARTICLE 03 : TEXTES DE REFERENCES

La présente Convention Cadre est régie, dans toutes ses dispositions par la législation et la règlementation algériennes.

ARTICLE 04 : AXES DE COOPERATION

Les Parties conviennent que les axes de coopération concernent d'une part, le déploiement des solutions R&D à échelle industrielle et d'autre part le Programme de Partage de Compétences.

4.1- La coopération, objet de la présente Convention Cadre, vise la conduite d'actions conjointes et concertées notamment en matière de :

- Direction des travaux de recherche scientifique et du développement technologique;
- Prise en charge des étudiants de l'USTO dans le cadre des activités pédagogiques telles que stages ou parrainages, dans le domaine qui intéresse SONATRACH ;
- Participation de la SONATRACH à l'élaboration des programmes de formation et de recherche présentant un intérêt commun ;
- L'accueil d'enseignants-chercheurs, chercheurs ou de doctorants, pour développer des pratiques pédagogiques innovantes, dans l'enseignement supérieur dans le domaine qui intéresse SONATRACH ;
- Constitution d'équipes mixtes de chercheurs autour de projets communs ;
- Études de modification, d'intégration, d'adaptation et de modernisation des systèmes ;
- Études, conception et réalisation de produits nécessaires à la mise en œuvre des projets de recherche scientifique et de développement technologique ;
- Maintenance et réparation des systèmes en dotation ;
- Formations spécifiques en rapport avec les projets et programmes qui seront initiés en commun, de formations de post-graduation spécialisée ainsi que de stages de courte durée ;
- Contribution aux actions d'encadrement du personnel stagiaire des deux Parties dans le cadre des formations initiées ;
- Réalisation des essais et des analyses de produits au niveau des laboratoires des deux parties dans le domaine de l'énergie, chimie, géologie, physique, ... etc.
- Séjours en laboratoires du personnel des Parties ;
- Détachement des spécialistes des Parties pour dispenser des cours en stages bloqués de courtes durées se rapportant aux projets ou programmes d'intérêt commun ;
- Organisation de séminaires et rencontres scientifiques ou pédagogiques en relation avec les domaines d'intérêt commun.

4.2- Dans le cadre de ces actions, les Parties conviennent de :

- Faciliter l'accès réciproque aux ressources et moyens de recherche respectifs : laboratoires, documentation scientifique et technique ;
- Prendre en charge, chaque partie en ce qui la concerne, l'acquisition d'équipements spécifiques dans le cadre de Contrats Spécifiques ;
- Œuvrer au transfert mutuel de technologies et du savoir-faire résultants des activités conjointes ;
- Promouvoir la valorisation des résultats obtenus et des compétences scientifiques et techniques constituées ;
- Encourager les espaces d'échanges et de concertation entre experts et chercheurs sur les perspectives de coopération et de développement dans les domaines d'intérêt commun.

ARTICLE 05 : DUREE DE LA CONVENTION CADRE

La présente Convention Cadre est conclue pour une durée de cinq (05) années, renouvelables par commun accord.

ARTICLE 06 : MISE EN ŒUVRE DE LA CONVENTION CADRE

Les Parties désigneront des représentants chargés de coordonner la mise en œuvre de la présente Convention Cadre.

Les Parties procèderont à l'identification des projets entrant dans les axes de coopération définis à l'article 04 suscité ceux susceptibles d'être mis en œuvre conjointement.

Chaque projet ou action identifié, fera l'objet, en fonction de sa nature, d'un Contrat Spécifique qui tiendra compte de sa nature, devra être conforme aux principes énoncés par la présente Convention et définira les actions de recherche scientifique et du développement technologique à engager entre les Parties, ainsi que leurs modalités et conditions de mise en œuvre.

Chaque Contrat Spécifique doit obligatoirement définir :

I. Les spécifications techniques relatives aux travaux à réaliser ;
II. Les objectifs à atteindre ;
III. La composante humaine en charge des travaux ;
IV. La durée, les règles particulières régissant la confidentialité et la propriété ;
V. Les contributions matérielles et humaines respectives de chaque Partie.

En cas de contradiction manifeste entre l'une des dispositions d'un Contrat Spécifique et de la présente Convention Cadre, les dispositions du de la présente Convention prévalent.

Le cas échéant, le Contrat Spécifique peut être modifié et/ou complété par des avenants signés par les Parties.

ARTICLE 07 : FINANCEMENT

Dans le cadre de la réalisation de l'objet de la présente Convention Cadre, les Parties conviennent que chacune en ce qui la concerne prendra en charge ses frais et coûts engagés pour les projets de partenariat.

ARTICLE 08 : COMITE DE PILOTAGE

8.1. Un Comité de Pilotage sera mis en place, dans un délai de dix (10) jours à compter de l'entrée en vigueur de la présente Convention et pour l'intégralité de sa durée de validité.

Le Comité de Pilotage est composé de quatre (04) représentants de chaque Partie. Toute désignation fera l'objet de notification dans les termes de l'article 17 de la présente Convention Cadre.

8.2. Le Comité de Pilotage a pour mission principale de superviser la mise en œuvre de la présente Convention, ainsi que des actions et projets objet des Contrats Spécifiques.

Le Comité de Pilotage est notamment chargé de :

- Arrêter le programme de mise en œuvre des actions et projets définis à l'article 04 de la présente Convention Cadre en :
  * Validant les actions à mener dans le cadre de ces projets ;
  * Arrêtant les besoins en financement ;
  * Soumettant le projet de Contrat Spécifique aux représentants habilités des Parties pour validation et signature ;
  * Approuvant les Projets achevés.
- Etablir des comptes rendus périodiques aux managements des Parties sur l'avancement de chaque projet ;
- Etablir un rapport périodique sur le déroulement des actions inscrites dans le cadre de la Convention Cadre ;
- Proposer la modification de la présente Convention Cadre en cas de nécessité ;

8.3. La présidence du Comité de Pilotage est assurée de manière alternée entre les parties de façon annuelle.

Le Comité de Pilotage désigne parmi ses membres un Secrétaire.

Le Comité de Pilotage établira, dès sa première réunion, son propre règlement intérieur.

Le Comité de Pilotage devra se réunir au moins deux (02) fois par an.

ARTICLE 09 : CONFIDENTIALITE

Toutes les données et informations de toutes natures échangées entre le Parties lors de l'exécution de la présente convention et/ou des contrats spécifiques ou en leurs occasions respectives, ainsi que les rapports du Comité de Pilotage ou autres comptes rendus, Procès-Verbaux ou documents en lien avec la coopération, y

compris le contenu de la présente Convention-Cadre, obtenus ou reçus par l'une des Parties dans le cadre de la présente Convention-Cadre et/ou d'un Contrat spécifique sont réputées confidentielles (Informations Confidentielles).

Chacune des Parties s'engage à ne pas divulguer de quelque façon que ce soit, ni à utiliser à d'autres fins que celles portées à la présente Convention sans l'accord préalable écrit de l'autre Partie, les Informations Confidentielles.

Cette disposition est sans effet si la Partie concernée peut apporter la preuve :

- Qu'elle avait déjà connaissance de façon légale des Informations Confidentielles avant la date de leur réception de la Partie divulgatrice ;
- Que ces informations ont fait l'objet d'une publication ou d'une communication autorisée par la Partie divulgatrice et/ou un de ses employés ;
- Qu'elles ont été reçues d'un tiers ayant le droit d'en disposer ;
- Qu'elles sont dans le domaine public ou ont été mises dans le domaine public par un tiers qui ne les aura pas reçus de la Partie réceptrice.

Par ailleurs, chacune des Parties est en droit de divulguer des Informations Confidentielles à ses propres dirigeants, salariés, préposés, agents et sous-traitants dont la connaissance des Informations Confidentielles est nécessaire à leur intervention au titre de la présente Convention Cadre sous réserve que la personne récipiendaire de l'Information Confidentielle soit informée de son caractère strictement confidentiel et s'oblige au respect des obligations en découlant dans des conditions non moins contraignantes que celles imposées aux Parties.

Aucune Partie ne pourra communiquer et/ou révéler les Informations Confidentielles de l'autre Partie à une personne ou à une entité tierce qu'après obtention de son accord préalable (qui ne peut être refusé sans juste motif) et sous réserve de leur imposer une obligation de confidentialité non moins contraignante que celle à laquelle elle est elle-même soumise.

Aucune publication, diffusion de rapports, de documents, communications, de résultats, savoir-faire et tous documents et ou informations issues des actions engagées dans le cadre de la présente Convention Cadre ne pourra être effectuée par l'une des Parties sans l'accord préalable et écrit de l'autre Partie.

Les termes de confidentialité spécifiques à chaque domaine de coopération seront définis dans les Contrats Spécifiques.

ARTICLE 10 : PROPRIETES

10.1- Nonobstant les dispositions de l'article 09 ci-dessus, les données nécessaires à la réalisation de chaque projet identifié demeureront la propriété de la Partie qui les fournit.

Chacune des Parties s'engage à mettre à la disposition de l'autre Partie les données dont elle dispose et qu'elle juge utile pour l'exécution de la présente Convention Cadre et de ces Contrats Spécifiques.

Sauf accord contraire, chacune des Parties conserve la propriété des résultats de ses recherches et développements propres effectués antérieurement à la prise d'effet de la présente Convention Cadre et/ou en dehors du cadre de la présente Convention Cadre.

Les données techniques fournies par une Partie dans le cadre de la présente Convention et /ou des Contrats Spécifiques pour les besoins de leur exécution restent, sauf accord contraire, la propriété exclusive de ladite Partie et ne peuvent faire l'objet de dépôt éventuel de titre de propriété sur ces données par l'autre Partie ou servir comme base à une éventuelle revendication de propriété.
Les droits de propriété des technologies, développements, inventions, dessins et/ou procédés obtenus antérieurement à la présente Convention-Cadre et le cas échéant des améliorations apportées dans le cadre des actions objet de la Convention-Cadre qui sont utilisés et/ou développés par l'une des Parties lors de l'exécution des actions et/ou qui pourraient résulter de l'exécution des actions conformément à la présente Convention-Cadre, resteront et seront, sauf accord contraire, la propriété exclusive de cette Partie. Les technologies, développements, inventions, dessins et procédés concernés par cette disposition seront exhaustivement listées dans les Contrats Spécifiques.
Les droits concernant les résultats des travaux obtenus dans le cadre de chaque action seront définis dans le cadre des Contrats Spécifiques.

Les résultats des travaux obtenus conjointement dans le cadre de chaque action, brevetables ou non, seront la propriété conjointe des Parties, au prorata de leurs apports intellectuels, matériels et financiers respectifs.

Les modalités de protection par un titre de propriété intellectuelle (tel qu'un brevet) et les droits d'exploitation portant sur ces résultats seront précisés dans les Contrats Spécifiques.

Les Parties pourront toutefois d'un commun accord décider de déroger à ce principe de copropriété dans les Contrats Spécifiques.

ARTICLE 11 : RESPONSABILITES

Le personnel de chaque Partie appelé à suivre ou à mener des activités de recherche dans les laboratoires sites et/ou installations de l'une ou l'autre Partie sont astreints au respect de leur règlement intérieur.

Sauf faute lourde ou intentionnelle suite au non-respect des engagements liés à la confidentialité et à la propriété intellectuelle tels qu'édicté dans les articles 09 et 10 ou des engagements contractuels assignés dans les contrats spécifiques, chacune des Parties renonce à tout recours contre l'autre Partie pour les dommages ou accidents subis par son personnel.

En cas de dommages intentionnels avérés, la Partie dont le personnel est mis en cause supportera la charge des dommages subis conformément à la règlementation en vigueur.

Les termes de responsabilité spécifiques à chaque domaine de coopération seront définis dans les Contrats Spécifiques.

ARTICLE 12 : RESILIATION

Chaque Partie se réserve le droit de résilier la présente Convention Cadre en informant l'autre Partie par écrit au moins trois (03) mois à l'avance.

Dans ce cas, aucune des Parties n'aura le droit de réclamer à l'autre Partie de dédommagement ou intérêt.

Sauf accord contraire écrit des Parties, la résiliation et/ou l'expiration de la présente Convention-Cadre n'affecteront pas les Contrats Spécifiques en cours d'exécution qui demeureront en vigueur et continueront à produire leurs effets jusqu'à l'achèvement complet des travaux.

Il demeure entendu qu'aucun Contrat Spécifique ne pourra être conclu ultérieurement à la notification de résiliation de la présente Convention.

ARTICLE 13 : REGLEMENT DES DIFFERENDS

Les Parties conviennent de régler à l'amiable tous litiges ou différends qui peuvent survenir au cours de l'interprétation et/ou de l'exécution de la présente Convention Cadre.

A défaut d'accord à l'amiable dans un délai de trente (30) jours, le litige sera soumis au Président Directeur Général du groupe SONATRACH.

ARTICLE 14 : FORCE MAJEURE

On entend par force majeure, pour l'exécution de la présente Convention Cadre, tout acte ou événement imprévisible, irrésistible et indépendant de la volonté des Parties, qui a pour effet de rendre impossible l'exécution de toute ou partie des obligations contractuelles.

Au cas où surviendrait un événement qui constituerait un cas de force majeure, la durée de la Convention Cadre ainsi que les délais éventuellement reportés seront prorogés du temps correspondant à la durée de la suspension des obligations résultant de la survenance du cas de force majeure.

La Partie qui invoque le cas de force majeure devra immédiatement après la survenance d'un tel cas de force majeure, adresser à l'autre Partie une notification (e-mail), fax, télégramme ou télex confirmé par lettre recommandée express avec accusé de réception. Cette notification devra être accompagnée de toutes les informations circonstanciées utiles et intervenir au plus tard dans les sept (07) jours à compter de la date de survenance de l'évènement sus cité.

Tout retard pour un cas de force majeure non notifié, dans les conditions et formes désignées ci-dessus, ne sera en aucune façon retenu pour le décompte du délai contractuel.

Dans tous les cas, la Partie empêchée devra prendre toutes les dispositions utiles pour assurer, dans les plus brefs délais, la reprise de l'exécution des obligations affectées par le cas de force majeure.

Si le cas de force majeure persiste au-delà de trente (30) jours, les Parties se rencontreront pour adopter une solution conforme à leurs intérêts réciproques.

ARTICLE 15 : CARACTERE NON ENGAGEANT

Dans le cadre de cette coopération, les relations entre les Parties seront régies par les dispositions de la présente Convention Cadre.

Sans préjudice des dispositions des articles 09, 10 et 11 ci-dessus, les Parties conviennent que la présente Convention Cadre ne peut être considérée comme un document engageant, obligeant les Parties à conclure des Contrats Spécifiques ou leur accordant un quelconque droit.

ARTICLE 16 : MODIFICATION

Toute modification de la présent Convention Cadre devra être formalisée par un avenant écrit signé par les Parties et qui sera conclu dans les mêmes conditions et formes que la présente Convention Cadre.

ARTICLE 17 : NOTIFICATION

Toute notification entre les Parties, pour les besoins de la présente Convention Cadre, pour être valable, doit intervenir par courrier avec accusé de réception aux adresses suivantes :

Pour SONATRACH / DC R&D :

Le Directeur Central Recherche et Développement

Adresse : Avenue du 1er Novembre, Boumerdès.

Téléphone : (213) 024 79 11 19

Fax : (213) 024 79 10 62

Email : sec.dcrd@sonatrach.dz

Pour l'USTO-MB

Vice-Recteur des relations extérieures à l'USTO-MB

Adresse : El M'naouar BP 1505, Bir El Djir 31000 Oran-Algérie.

Téléphone : (213) 41 61 71 46 / (213) 41 62 71 60

Tél/Fax : (213) 41-62-71-45

E-mail : vrrelex@univ-usto.dz

Chaque Partie est tenue d'informer l'autre Partie par notification écrite, de tout changement d'adresse, sous peine d'inopposabilité.

ARTICLE 18 : ENTREE EN VIGUEUR

La présente Convention Cadre entre en vigueur à compter de la date de sa signature par les Parties.

La présente Convention Cadre est établie en six (06) exemplaires originaux paraphés et signés, en langue française, dont trois (03) exemplaires pour chacune des Parties.

Fait à Oran, le 04 SEPT 2024

P/SONATRACH	P/l'USTO-MB
MONSIEUR LE DIRECTEUR CENTRAL RECHERCHE ET DEVELOPPEMENT	MONSIEUR LE RECTEUR DE L'USTO-MB
Mustapha Mohamed BENAMARA	Ahmed HAMOU

CONVENTION CADRE de PARTENARIAT

Entre d'une part:

L'Université des Sciences et de la Technologie d'Oran-Mohamed BOUDIAF (USTO-MB) représentée par son Recteur Professeur HAMOU Ahmed l'Université des Sciences et de technologie d'Oran Mohamed Boudiaf USTO-MB, sise BP 1505 Oran El M'Naouer Bir El Djir à Oran, Algérie.

Et d'autre part:

L'entreprise OraNovia sise au 31 Boulevard des Lions à Oran, représentée par son Directeur Général M. BENZAGHOU Karim.

Préambule

L'USTO-MB, dans le cadre de ses missions de service public, œuvre pour l'intégration de ses jeunes diplômés dans le monde du travail en leur assurant une formation de qualité et des stages d'induction dans les entreprises partenaires de la région, tout au long de leur cursus de formation.

Ainsi, **L'USTO-MB** et **L'entreprise OraNovia** décident de conjuguer leurs efforts et de rechercher une complémentarité dans l'action par des échanges, de susciter de nouvelles initiatives, d'instaurer un dialogue sur le long terme, dans un esprit d'ouverture et de réciprocité.

Il est entendu entre les parties, qu'aucune contrepartie pécuniaire n'est envisagée et que le cadre de ces échanges et collaboration est à titre gracieux.

Il a été convenu et arrêté ce qui suit :

ARTICLE 01: OBJET DE LA CONVENTION

La présente convention est une convention cadre, ayant pour objet de fixer les conditions générales et les modalités de mise en œuvre d'un partenariat entre **l'USTO-MB** et **OraNovia**

ARTICLE 02 : ENGAGEMENTS DES PARTIES

Au titre de ce partenariat, les parties s'engagent à :

2.1- Engagements de l'USTO-MB :

-prise en compte et respect des dispositions légales, réglementaires et des procédures administratives applicables dans le cadre de l'exécution de la présente convention ;
-respect strict et rigoureux des règles applicables au sein de l'entreprise concernant la santé, la sécurité et la qualité, définies et faisant partie intégrante de cette convention, lors de visites, stages, utilisations d'équipements dans l'Entreprise.
-information les étudiants des événements de l'entreprise, liés au recrutement et à l'insertion professionnelle ;
-susciter la participation de l'entreprise aux jurys de sélection ;

-organisation d'actions de formation en faveur du personnel des unités de production ;

-engagement à étudier toute demande de création de formation ad hoc en formation continue pour l'entreprise ;
- mise à la disposition de l'entreprise les listes des étudiants sortants (diplômés) classés par ordre de mérite (Licence et Master) ;
- participation des personnels de l'entreprise, conformément à la réglementation en vigueur, aux formations diplômantes, qualifiantes et Post-graduation assurées par l'USTO- MB;
- invitation régulière des experts de l'entreprise à prendre part aux journées d'informations et aux manifestations scientifiques organisées par **l'USTO-MB** ;

-autorisation de **l'entreprise** à programmer des journées d'informations au sein des structures de **l'USTO-MB**, et à animer des conférences et séminaires qui s'inscrivent dans le cadre des objectifs pédagogiques prédéfinis par l'équipe enseignante tout en permettant aux étudiants d'y assister ;

- proposition des sujets de thèse intéressant l'entreprise ;

- mise à la disposition **de l'entreprise** des espaces dans les organes de communication de **l'USTO-MB** (Ex. le site Web, facebook, ...) pour communiquer avec les étudiants ;
-autorisation d'utiliser les équipements et supports de recherche de façon réciproque ;

2.2- Engagements de l'entreprise :
-Co-construction de programmes pédagogiques (Licences et Masters Pro) ;

-préparation aux métiers de l'industrie ;
-formation continue, validation des acquis de l'expérience ;
- communication des offres d'emploi ;
- coopération scientifique, valorisation des chercheurs ;
-signature des cahiers de charges des stages professionnels au profit des étudiants ;
-mise en place d'un cadre propice à la promotion de la thèse en entreprise et aux activités de prestations de service telles que la maintenance, le contrôle qualité, le consulting etc.

ARTICLE 03 : EVALUATION DU PARTENARIAT

Les parties se réuniront, minimum, une fois par an afin d'établir le bilan de l'année écoulée et définir par avenant les objectifs de l'année suivante ainsi que les actions qui en découlent pour les parties.
Il est mis en place un Comité de Partenariat qui a pour mission d'organiser les actions relations Université/Entreprise qui constituent l'objet du partenariat et de suivre leur développement.

Le Comité de Pilotage est constitué de:
Pour l'USTO-MB :

Pr Naima Djabaria MEROUFEL
Pr Bachir DJEBBAR
Pr Latifa DEKHICI

Pour l'Entreprise :
M. Karim BENZAGHOU (Directeur Général et Architecte Solutions)
M. Mohammed Ismail HAI (Technical Lead Microsoft Business Application)
M. Imad Eddine OULHACI (Technical Lead Microsoft Business Application)

ARTICLE 04 : Statut des personnels

Les personnels de l'USTO-MB et de l'entreprise œuvrant dans le cadre de la présente convention demeurent salariés de leur propre employeur et leur protection sociale assurée selon les règles habituelles à chaque partie.
Les intéressés seront soumis aux règlements intérieurs des établissements qui les accueillent.

ARTICLE 05 : CONFIDENTIALITÉ

Les Parties conviennent que le présent Accord et les sujets que les Parties seront amenées à traiter dans ce cadre pourront faire l'objet d'une annonce publique par voie de presse (communiqué, article, conférence…) ou par tout autre moyen de communication.

Toutefois, préalablement à toute communication, chacune des Parties devra obtenir l'accord préalable écrit de l'autre Partie quant à son contenu, à son mode de diffusion ainsi qu'à la durée et à l'étendue géographique de sa diffusion.

Nonobstant ce qui précède, les Parties s'engagent à ne divulguer aucune information déclarée comme étant de nature confidentielle par son propriétaire et n'étant pas destinée à l'usage public.

Cette obligation de confidentialité s'appliquera pendant toute la durée du présent accord et les cinq (5) années qui suivent sa cessation pour quelque cause que ce soit.

Chaque Partie s'engage en conséquence à faire respecter cette obligation par son personnel et ses éventuels partenaires qui seront amenés à participer aux sujets qui seront traités par **L'USTO-MB** et **l'Entreprise**.

Les deux parties conviennent de respecter le caractère confidentiel des résultats de certaines de leurs recherches et s'engagent à ne divulguer leurs contenus sans accord préalable de l'autre partie.

ARTICLE 06 : COMMUNICATION

Les parties se concerteront pour la promotion et la communication de ce partenariat et des actions qui en découlent.
Les logos et sigles devront respecter les chartes graphiques de chacune des parties. Leur utilisation doit être conforme aux règles d'éthique en usage.
Les documents et supports comportant les logos, sigles et mentions relatives au partenariat devront-être communiqués préalablement à leur diffusion à chacun des partenaires pour information et aval le cas échéant (respect du droit des marques et de la propriété intellectuelle.

ARTICLE 07 : LITIGES

En cas de litiges, les partenaires s'engagent à régler à l'amiable, par voie de médiation ou par tout autre moyen, à l'exclusion de tout recours aux tribunaux, les différens qui pourraient survenir à l'occasion de la mise en œuvre de la présente convention ou de ses avenants.

ARTICLE 08 : ENTRÉE EN VIGUEUR ET DURÉE DE LA CONVENTION

La présente convention est rédigée en quatre exemplaires, entrera en vigueur à compter de la date de sa signature par les deux parties pour une période de trois (3) années.

Si, en cas de la dénonciation anticipée, une opération définie par voie d'avenant à la présente convention était en cours, la résiliation ne deviendra effective qu'à la date d'achèvement de cette opération. En cas de cessation d'activité, celle-ci serait immédiate. Toute modification de la présente convention nécessite l'approbation écrite des représentants des trois parties.

Fait à Oran, le : 26 MAI 2025

Pour l'USTO-MB	Pour l'Entreprise OraNovia
Le Recteur :	Directeur Général :
Pr émérite. HAMOU Ahmed	M. BENZAGHOU Karim

OraNovia
Gérant
Karim BENZAGHOU
EURL OraNovia
POS 50 IMMEUBLE C4 RESIDENCE MIRABELLE
LOT 1035 BIR EL DJIR ORAN
karim.benzaghou@oranovia.com

Article 09 :Dispositions finales

La présente convention entrera en vigueur à compter de la date de sa signature par les deux (02) parties et sera valable jusqu'à la réalisation des objectifs cités ci-dessus.

A cette date, à moins que les Parties n'en aient conjointement convenus différemment aux termes d'un avenant, la présente convention ce sera pour l'avenir de produire ses effets.