• UNIVERSITÉ LIBANAISE •
• UNIVERSITÉ SAINT-JOSEPH •

MASTER
Télécoms, Réseaux et Sécurité

Option recherche : Réseaux

Option spécialisée : Ingénierie de la Cybersécurité

En partenariat avec :

_____

Télécom ParisTech, France
La Banque Centrale du Liban

_____

Renseignements et Retrait des dossiers:

http://ulfg.ul.edu.lb/master2/master6.aspx
http://www.cimti.usj.edu.lb/files/master_TRS.html

Faculté de Génie, Université Libanaise
Campus de Hadath
Tel : (05) 463 489

Faculté d'Ingénierie, Université Saint Joseph (USJ)
Mar Roukos, Mkalles
Tel : (01) 421317

_____

INFORMATIONS GÉNÉRALES

Les systèmes de télécommunications apportent aujourd'hui une dimension nouvelle à notre société avec des enjeux technologiques, économiques et sociologiques. Les réseaux de communication et leur sécurité ainsi que leurs applications historiques font désormais l'objet de nombreuses initiatives et nourrissent une forte demande sur le marché de l'emploi en ingénieurs spécialistes et en chercheurs qualifiés. Celle-ci va se renforcer à l'avenir avec la concurrence amplifiée par la dérégulation, l'apparition de nouveaux métiers requérant une main d'œuvre qualifiée, ainsi que par les développements technologiques et économiques autour des services sur l'Internet et de la cybersécurité, autour des mobiles, des réseaux privés et des opérateurs traditionnels.

OBJECTIF SCIENTIFIQUE ET PEDAGOGIQUE

Le mastère Télécoms, Réseaux et Sécurité forme des ingénieurs, des chercheurs en réseaux et sécurité pour maîtriser l'environnement global lié aux réseaux de télécommunications et les problématiques de sécurité.
Le mastère Télécoms, Réseaux et Sécurité offre aux étudiants deux options (parcours) : une **option spécialisée** qui se focalise sur l'ingénierie de la cybersécurité pour devenir des spécialistes de sécurité. Une **option recherche** pour devenir des chercheurs dans des domaines tels que la sécurité, la conception de réseaux et de systèmes de télécommunications, l'administration des réseaux, la transmission de flots multimédias et l'Internet du futur. Cette formation permet également aux étudiants qui le désirent de préparer une thèse doctorale dans ce domaine.

Ce Master vise à former :

- des spécialistes de haut niveau de la cybersécurité nécessaires dans les diverses administrations concernées et bureaux d'études,
- des enseignants et des chercheurs,
- des chercheurs étrangers: en raison de l'importance des problèmes abordés, l'ouverture à des étudiants étrangers du bassin méditerranéen peut amener une synergie favorable à une meilleure utilisation commune de la ressource.

C'est un diplôme interuniversitaire au Liban, sanctionnant une formation à laquelle des établissements réputés apportent leur collaboration et leurs moyens pédagogiques et scientifiques.

Deux facultés appartenant à deux universités libanaises : La **Faculté de Génie** de *l'Université Libanaise*, et la **Faculté d'Ingénierie** de *l'Université Saint-Joseph* agissent en commun, sous l'égide du *Ministère de la Culture et de l'Enseignement Supérieur*, pour co-habiliter en partenariat avec *Télécom ParisTech et la banque centrale du Liban* la formation de haut niveau distribuée dans le cadre de ce Master.

ORGANISATION GENERALE DU MASTER

Le master est une formation d'une durée de deux semestres MS1 et MS2 de 30 crédits chacun. Le programme dispense les enseignements des semestres MS1 et MS2, comprenant :

- des enseignements théoriques et pratiques,
- un stage en entreprise pour le parcours spécialisé et un stage de recherche pour le parcours recherche donnant lieu à la rédaction d'un mémoire et à la soutenance d'une thèse professionnelle

Les stages et travaux de recherche se dérouleront soit au Liban dans les entreprises ou laboratoires, soit dans un laboratoire d'un établissement extérieur. La responsabilité scientifique du stage est assurée conjointement par le ou les enseignants - chercheurs qui dirigent le stage. Les stages faits au Liban sont supervisés par les deux facultés libanaises sur des thèmes agréés par le Comité de suivi du Master (CS).

Ce stage, d'une durée minimale d'un semestre (MS2), a pour objectif de développer chez l'étudiant l'ensemble des compétences nécessaires à un spécialiste :

- recherche bibliographique.
- analyse critique de l'état de l'art.
- propositions et implémentations des solutions
- propositions et débouchés sur des travaux de thèse (pour les étudiants ayant choisi une orientation recherche)

Le stage fait l'objet d'un mémoire écrit et d'une soutenance publique. Le mémoire comporte une partie bibliographique et une partie technique.

L'évaluation du stage tient compte de trois éléments :

- Évaluation de l'initiative scientifique du stagiaire.
- Évaluation du mémoire écrit.
- Évaluation de la soutenance orale.

ADMISSION

Le mastère est une formation Bac+6, sont autorisés à déposer les dossiers de candidature :

- Les ingénieurs diplômés,
- Les titulaires d'un Master professionnel ou recherche en Génie Electrique, Réseaux, Informatique, Télécommunications,
- Les titulaires d'un diplôme reconnu équivalent.

La sélection des candidats est faite par un jury d'admission dans la limite des places disponibles. Le jury d'admission décidera pour chaque candidature les matières et modules validés en fonction du cursus et des résultats préalablement obtenus.

LE DIPLOME

Le diplôme Master en **"Télécoms, Réseaux et Sécurité" option spécialisée** ou bien **option recherche** est délivré aux étudiants admis ayant subi avec succès les contrôles portant sur les enseignements et la soutenance de leur mémoire, tels que définis par le règlement intérieur.

Le diplôme Master est décerné sous les sceaux de l'Université Libanaise et de l'Université Saint Joseph, il est reconnu par les établissements partenaires étrangers.

RÈGLEMENT DU DIPLÔME

1. Langue d'enseignement.
L'enseignement se fera en français. La maîtrise de cette langue est donc nécessaire.

2. Contrôle des connaissances
Le Master **Télécoms, Réseaux et Sécurité** est délivré aux candidats qui ont subi avec succès les contrôles portant sur les enseignements théoriques et pratiques et qui justifient d'un niveau suffisant lors de la préparation et de la soutenance du mémoire. En cas d'absence, il n'est pas prévu de rattrapage des examens. En cas d'accident grave, dûment et sérieusement justifié, le cas sera examiné par le jury de fin d'année en vue de prendre les mesures jugées convenables.

3. Présences
Toutes les activités d'enseignement sont obligatoires. Des contrôles sont périodiquement effectués. Pour toute matière, si le total des absences injustifiées est supérieur à 30% du nombre total d'heures programmées, l'étudiant ne peut se présenter au contrôle relatif à cette matière. Dans ce cas l'étudiant ne peut se présenter à l'examen, obtient la note zéro (ECTS : F). Si par suite de cette mesure, l'étudiant rate plus de trois contrôles, il est considéré comme démissionnaire du programme du Master.

4. Conditions

A chaque matière est affectée une note sur 20. Une moyenne générale des modules théoriques est calculée à partir des notes des matières du semestre, pondérées par le nombre de crédits. Un système de rappel est appliqué pour toute matière où l'étudiant a obtenu une note inférieure à 10/20. L'étudiant ne fera pas un rappel pour la matière dont la note est entre 8 et 10 si la moyenne générale est supérieure ou égale à 11/20. Suite aux rappels un jury est réuni et arrête les résultats.
Les modules théoriques sont validés si :

a. les notes de toutes les matières sont supérieures à dix.
b. Si dans certaines matières la note est entre 8 et 10, la moyenne générale de réussite est de 11/20.

Sont autorisés à présenter le mémoire les étudiants qui ont validé les modules théoriques. La priorité dans le choix des stages est fonction de la moyenne générale.

Le mémoire est validé si la note est supérieure ou égale à 12/20.

5. Diplôme.

Les études sont sanctionnées par la délivrance d'un Diplôme de Master en **Télécoms, Réseaux et Sécurité**, **option spécialisée** ou bien **option recherche** lorsque le candidat valide toutes les matières des 2 semestres MS1 et MS2.

Une moyenne générale est établie en appliquant une pondération de 50% pour la moyenne du semestre MS1 et de 50% pour le mémoire MS2). En fonction de quoi, les mentions suivantes sont accordées :

- de 12/20 à 13,99/20 : Assez Bien
- de 14/20 à 15,99/20 : Bien
- à partir de 16/20 : Très Bien

CONDITIONS D'INSCRIPTION

Les admissions se font sur dossier. Celui-ci comprendra :

- Copies certifiées conformes des diplômes obtenus[1] dont le baccalauréat
- Copies certifiées conformes des notes obtenues au cours des études universitaires[1].
- Liste des enseignements suivis au cours de la scolarité.
- Extrait d'état civil.
- Trois photos d'identité portant le nom et le prénom du candidat au verso.
- Curriculum Vitae du candidat.
- Copie des certificats de travail et attestation d'expérience professionnelle du candidat.
- Engagement précisant la maîtrise de la langue française (rédigée par le candidat s'il n'a pas d'attestation officielle).

(1)- Le candidat est tenu de présenter pour constat, les documents originaux le jour de l'inscription.

Les dossiers seront examinés par le CS qui établira la liste des candidats admis à suivre cette formation. Les candidats retenus pourraient être soumis à un entretien avant leur admission finale. L'ensemble de cette formation sera distribuée en **langue française**. En cas de besoin, le CS pourra vérifier le niveau de langue française du candidat et exiger de lui le cas échéant, une mise à niveau linguistique. Le dossier de candidature est à retirer et à déposer au :

Faculté de Génie, Université Libanaise
Campus de Hadath
Tel : (05) 463 489

Faculté d'Ingénierie, Université Saint Joseph (USJ)
Mar Roukos, Mkalles
Tel : (01) 421317

DROITS D'INSCRIPTION

Le montant des droits d'inscription est fixé à 1 800 000 livres libanaises (incluant les droits d'inscription aux deux universités libanaises partenaires). Aucun remboursement ne sera effectué en cas d'abandon des études.

ÉTUDES DOCTORALES

Certains étudiants ayant choisi une orientation recherche et ayant obtenu avec une bonne appréciation de leur Master, pourront intégrer la préparation d'une thèse de doctorat (en co-tutelle entre le Liban et un établissement francophone) et présenter auprès de l'AUF ou du CNRSL une demande pour l'obtention d'une bourse de thèse doctorale. Pour les étudiants ayant suivi l'option spécialisée, ils peuvent aussi intégrer la préparation d'une thèse de doctorat suite à une excellente appréciation de leur Master.

ORGANISATION DES ENSEIGNEMENTS

Les matières des semestres MS1 et MS2 sont :

Code	Module	C+TPC	Crédits
MTRS01S1	**Architectures des réseaux de données**	**24h**	**3**
MTRS02S1	**Modélisation des réseaux**	**24h**	**3**
MTRS03S1	**TCP/IP avancé & QoS**	**18h**	**3**
MTRS04S1	**Programmation Réseau**	**18h**	**3**
MTRS05S1	**Cryptographie**	**24h**	**3**
MTRS06S1	**Sécurité dans les réseaux**	**18h**	**3**
Option recherche : Réseaux			
MTRS07S1	**Architectures de réseaux télécom fixes et mobiles**	**18h**	**3**
MTRS08S1	**Techniques radio avancées**	**18h**	**3**
MTRS09S1	**Réseaux et Services télécom**	**18h**	**3**
MTRS10S1	**Dimensionnement et planification des réseaux**	**18h**	**3**
Option Spécialisée : Ingénierie de Cybersécurité			
MTRS11S1	**Sécurité des systèmes d'information**	**18h**	**3**
MTRS12S1	**Modèles de sécurité**	**24h**	**3**
MTRS13S1	**Sécurité des logiciels**	**18h**	**3**
MTRS14S1	**Cybercriminalité et investigation numérique**	**18h**	**3**
MTRS01S2	**Mémoire de stage**	**0h + 300h**	**30**

MTRS01S1. Architectures des réseaux de données - C+TPC 24h, 3 crédits
Définition des mécanismes de communication. Concepts réseau : commutation, contrôle de flux et de congestion, contrôle d'erreur. Architecture OSI et fondamentaux de la pile TCP/IP. Protocoles de routage (RIP, OSPF, BGP). Adressage et gestion de groupe multipoint (IGMP). Routage multipoint (DVMRP, PIM). Introduction à la commutation et à la structure des commutateurs/routeurs. Architecture des réseaux locaux. VLAN et leurs applications. Architecture de l'Internet du futur, Technologies du réseau Backbone, Réseaux optiques, commutation optiques. TP Simulation de Réseaux. Mini-projet.

MTRS02S1. Modélisation des réseaux – C+TPC 24h, 3 crédits
Chaînes de Markov (à temps discret et à temps continu). Processus de naissance et de mort. Formalisme files d'attente (notation de Kendall). Files markoviennes en particulier file M/M/1 et file M/M/C/C (Little, Erlang-B, Erlang-C). Files non markoviennes (M/G/1 et G/M/1). Réseaux de file d'attente. Réseaux à forme produit. Processus de modélisation du trafic (Poisson, Périodique, auto similaire). Modèles d'agrégation de trafic. Applications de modélisation.

MTRS03S1. TCP/IP avancé et QoS - C+TPC 18h, 3 crédits
Variantes de TCP. Protocoles pour la fiabilité et le contrôle de congestion pour le multipoint. Evolution IPv6. Mobilité IP. Multihoming et SCTP. Architecture de QoS, IntServ et RSVP, DiffServ, MPLS. Routage à qualité de service, Mécanismes de Gestion de flux (RED, WFQ, etc), Structure d'applications multimédias: vidéoconférences, téléphonie IP.

MTRS04S1. Programmation Réseau - C+TPC 18h, 3 crédits
Programmation et Architectures applicatives - Systèmes d'agents et multi-agents – Agents intelligents - Architectures peer-to-peer - Travaux Pratiques

MTRS05S1. Cryptographie - C+TPC 24h, 3 crédits
Rappel sur les Services de Sécurité. Historique de la Cryptographie. Algorithmes Symétriques, Asymétriques, Fonctions Hash. Mécanismes et Techniques Cryptographiques. Modes Cryptographiques. Standards PKCS. Enveloppes. PKI. Cartes à Puce. Cryptographie et ASN1. Cryptographie moderne (quantique). Les cours seront donnés dans le laboratoire cryptographique avec utilisation des Outils Cryptographiques pour mettre en œuvre les algorithmes symétriques, asymétriques, hash, modes cryptographiques, protocoles cryptographiques et dispositifs de sécurité.

MTRS06S1. Sécurité dans les réseaux - C+TPC 18h, 3 crédits
Techniques et architectures des réseaux. Attaques sur les réseaux. Services et domaines de la sécurité. Sécurisation des réseaux et solutions associées. Outils et équipements (cartes à puce) pour la sécurité. Etudes de cas réels pour la sécurisation des réseaux. Distribution de clés - PKI - Audit - Composants (TPM) - Applications: réseaux Ad-hoc, RFID, peer-to-peer, annuaire et messagerie électroniques, SMIME, etc. Sécurité dans les réseaux télécoms et paquets fixes et mobiles (GSM ,UMTS, WiMAX).

MTRS07S1. Architectures de réseaux télécom fixes et mobiles- C+TPC 18h, 3 crédits
Architecture fonctionnelle d'un réseau de télécommunications fixe/mobile. Réseaux d'accès à bande étroite filaire (RNIS, XDSL). Réseau sémaphore SS7. Protocoles du plan contrôle pour l'UNI. Signalisation Q.931. Architecture des réseaux mobiles (GSM, GPRS, UMTS). Hand-over, itinérance, itinérance internationale, signalisation liée à la mobilité MAP. Architecture des réseaux cellulaires LTE. E-UTRAN, QoS et Mobilité dans LTE. Interfonctionnement de systèmes, interface multi-mode.

MTRS08S1. Techniques radio avancées - C+TPC 18h, 3 crédits
Canaux de transmission radio mobile. Modèle de canal multi-trajet. Egalisation et synchronisation. Techniques de modulation à étalement de spectre. Techniques de modulation multi-porteuses (OFDM). Techniques d'accès multiples FDMA, TDMA. Techniques d'accès sans fil large bande, CDMA et OFDMA. Techniques multi-antennes (MIMO), Diversité de transmission/réception, Codage espace-temps. Allocation des ressources.

MTRS09S1. Réseaux et Services télécom - C+TPC 18h, 3 crédits
Principes et organisation du réseau intelligent IN. Modèle conceptuel du réseau intelligent. Exemples de services et leurs principaux composants fonctionnels, évolution des services. CAMEL (Customized Applications for Mobile network Enhanced Logic). Convergence fixe-mobile. Services multimédia. VoIP. Architecture IMS. Les services au-delà de la 3G. VHE.

MTRS10S1. Dimensionnement et Planification des réseaux - C+TPC 18h, 3 crédits
Problèmes d'évaluation de performance et de modélisation de systèmes de communication. Modèles du multiplexage. Réseaux à perte. Routage. Contrôle de flux. Contrôle d'admission. Dimensionnement du réseau d'accès et réseau cœur. Planification d'un réseau cellulaire - Cas du GSM et cas de l'UMTS - Dimensionnement d'un réseau cellulaire - Optimisation et technique de densification - Dimensionnement d'un réseau WiMAX. Introduction à la planification des réseaux B3G.

MTRS11S1. Sécurité des systèmes d'information - C+TPC 18h, 3 crédits
Mécanismes de base de la sécurité. Modèles et techniques d'authentification. Sécurité des mots de passe et techniques de craquage. Sécurité des bases de données. Sécurité des sites web. Sécurité et Cloud.

MTRS12S1. Modèles de sécurité - C+TPC 24h, 3 crédits
Méthodes d'évaluation du risques (NIST, EBIOS, MEHARI, OCTAVE) – Checklists et politique de sécurité (PCI DSS, SANS, ISO) - Organisation de la sécurité de l'information - Gestion des biens d'une entreprise - Sécurité des ressources humaines - Sécurité Physique et environnementale (PCI DSS, NIST, SANS, ISO) - Control d'accès (PCI DSS, SANS, ISO) - Gestion des Incidents et des événements (ISO, NIST) - Plan de continuité des activités (ISO, BCI) .
Aspects juridiques: Contexte juridique de la sécurité des systèmes d'information, Les obligations légales et réglementaires de sécurisation, Les aspects juridiques de la démarche de sécurisation.

MTRS13S1. Sécurité des logiciels - C+TPC 18h, 3 crédits
Analyse des vulnérabilités - Logiciels malveillants: principes, techniques, furtivité – retro ingénierie (Reverse Engineering) - techniques de détection - mesure de prévention - sécurité des systèmes d'exploitation - sécurité des applications mobiles.

MTRS14S1. Cybercriminalité et investigation numérique - C+TPC 18h, 3 crédits
Panorama de la cybercriminalité - Menaces et qualification juridique - Lutte contre la cybercriminalité et Droits et Libertés fondamentaux - Cybercriminalité et coopérations nationales et internationales - Droits et obligations des acteurs de la société de l'information - Crimes contre la personne: activités à caractère sexuel, Cyberbullying - Sécurité de l'information et intelligence économique - Impact économique de la cybercriminalité (blanchiment d'argent, cyber-fraudes, ..) - Réseaux sociaux: impacts pour l'entreprise, risques et responsabilités - Risques spécifiques aux paiements en ligne et réglementations - Investigation numériques: Introduction aux techniques d'investigation numériques (computer forensics), Panorama de la criminalistique, Missions et déroulement de l'expertise judiciaire, Interception des données sur le réseau Internet.

MTRS01S2 Mémoire de stage C 0 h, TPC 300 h, 30 crédits
Il constitue une initiation à un projet industriel ou bien aux techniques de la recherche. C'est la synthèse d'un travail de six mois dans l'entreprise ou dans un centre de recherche ou un laboratoire.