

• UNIVERSITÉ LIBANAISE •  
• UNIVERSITÉ SAINT-JOSEPH DE  
BEYROUTH •

**MASTER**  
**Télécoms, Réseaux et Sécurité**  
**Telecoms Networks and Security**

**Renseignements et Retrait des dossiers:**

**<http://www.ulfg.ul.edu.lb/master-sections/6>**  
**<https://fi.usj.edu.lb/esib/ded.html>**

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

**Faculté d'Ingénierie, Université Saint Joseph de Beyrouth (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 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 qui nécessitent 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 de télécommunications.

## 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. Les étudiants pourront par exemple devenir chercheurs dans des domaines tels que la sécurité, la conception de réseaux et de systèmes de télécommunications, l'administration des réseaux, la transmission de contenus 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 enseignants et des chercheurs,
- des spécialistes de haut niveau de la sécurité des réseaux et la cybersécurité nécessaires dans les diverses administrations concernées et bureaux d'études,
- 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 de Beyrouth* agissent en commun, sous l'égide du *Ministère de la Culture et de l'Enseignement Supérieur*, pour co-habiller en partenariat avec *Télécom ParisTech* la formation de haut niveau distribuée dans le cadre de ce Master.

## ORGANISATION GENERALE DU MASTER

Le Master comporte 120 crédits, répartis sur 4 semestres de 30 crédits chacun. Ce programme dispense les enseignements des deux derniers semestres. Ces deux semestres MS1 et MS2 de 30 crédits chacun, comprennent :

- des enseignements théoriques et pratiques,

- un stage de recherche donnant lieu à la rédaction d'un mémoire et à la soutenance devant un jury.

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 de continuer en thèse.

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**

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 DIPLÔME

Le diplôme Master 2 Recherche en "**Télécoms, Réseaux et Sécurité**" 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 de Beyrouth, 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 **Télécoms, Réseaux et Sécurité**, 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<sup>1</sup> dont le baccalauréat
- Copies certifiées conformes des notes obtenues au cours des études universitaires<sup>1</sup>.
- 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 de Beyrouth (USJ)**  
**Mar Roukos, Mkalles**  
**Tel : (01) 421317**

## DROITS D'INSCRIPTION

Le montant des droits d'inscription pour tous les étudiants est le montant officiel en Livres Libanaises à l'Université Libanaise et 1000 US Dollars à l'Université Saint-Joseph. Aucun remboursement ne sera effectué en cas d'abandon des études.

## ÉTUDES DOCTORALES

Certains étudiants ayant obtenu avec excellente appréciation 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 CNRS-L une demande pour l'obtention d'une bourse de thèse doctorale.

## ORGANISATION DES ENSEIGNEMENTS

Les matières des semestres MS1 et MS2 sont :

Code	Module	C+TPC	Crédits
MTRS01S1	Protocoles et services réseaux avancés	24h	3
MTRS02S1	Réseaux mobiles et cellulaires	24h	3
MTRS03S1	Cryptographie	21h	3
MTRS04S1	Modélisation des réseaux	21h	3
MTRS05S1	Optimisation pour les réseaux	18h	3
MTRS06S1	Cloud et Architectures applicatives	21h	3
MTRS07S1	Sécurité dans les réseaux	18h	3
MTRS08S1	Cybersécurité	24h	3
MTRS09S1	Réseaux sans fil	18h	3
MTRS10S1	Machine Learning pour les réseaux et la Cybersécurité	21h	3
MTRS01S2	Mémoire de stage	0h + 300h	30

### **MTRS01S1. Protocoles et services réseaux avancés - C+TPC 24h, 3 crédits**

Commutation, contrôle de flux et de congestion, contrôle d'erreur. Protocoles de routage (RIP, OSPF, BGP). Adressage et gestion de groupe multipoint (IGMP). Routage multipoint (DVMRP, PIM). 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, Service MPLS. Routage à qualité de service, Mécanismes de Gestion de flux (RED, WFQ, etc), VoIP.

### **MTRS02S1. Réseaux mobiles et Cellulaires- C+TPC 24h, 3 crédits**

Concepts et fonctions cellulaires dans les réseaux mobiles ; Standardisation et évolution des réseaux mobiles ; réseaux LTE et 4G (LTE-Advanced et LTE-Advanced Pro) : services, interface radio, architectures physique et protocolaire, canaux physiques, de transport et logiques, voix dans LTE, gestion des flux de données, gestion des ressources radio, gestion de la sécurité et évolutions du LTE vers le LTE-Advanced et le LTE-Advanced Pro ; avancées récentes dans les réseaux mobiles;

dimensionnement et planification radio des réseaux 4G ; pratiques de déploiement des réseaux mobiles; qualité de service et optimisation des réseaux mobiles ; C-RAN ; SDN ; Internet des objets cellulaire.

#### **MTRS03S1. Cryptographie - C+TPC 21h, 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.

#### **MTRS04S1. Modélisation des réseaux – C+TPC 21h, 3 crédits**

Introduction à la théorie de télé-traffic. Modèle de source sans mémoire (Bernoulli et Poisson) et étude du multiplexage et de l'accès multiple. Chaînes de Markov à temps discret et à temps continu. Introduction à la théorie des files d'attente). Files markoviennes de type M/M et applications à la modélisation dans les réseaux. Réseaux de file d'attente. Réseaux à forme produit. Modèles de trafic et d'agrégation de trafic. Files non markoviennes (M/G/1 et G/M/1). Problèmes d'évaluation de performance et de modélisation des systèmes de communication. Dimensionnement.

#### **MTRS05S1. Optimisation pour les réseaux - C+TPC 18h, 3 crédits**

Optimisation mathématique : formulation d'un problème d'optimisation, problème d'optimisation linéaire, problème d'optimisation non-linéaire convexe, problème d'optimisation en nombres entiers, problème d'optimisation non-linéaire non-convexe. Recherche de solution optimale : lagrangien, dualité, conditions d'optimalité, complexité, outils et logiciels pour l'optimisation.

Algorithmes : simplexe, branch and bound, gradient et sous-gradient, décomposition primale et duale, méta-heuristique. Optimisation multi-objectif : dominance, méthode scalaire, critère de Pareto et critère utilitariste. Optimisation et théorie des jeux : jeux non-coopératifs, fonction utilité et optimisation, équilibre de Nash, algorithme Best Response. Application de l'optimisation pour les réseaux : routage dans les réseaux, dimensionnement des réseaux, allocation de la bande passante et problèmes d'équité, ordonnancement dans les réseaux sans-fil, contrôle de puissance dans les réseaux sans-fil, sélection de l'accès sans-fil.

#### **MTRS06S1. Cloud et Architectures applicatives - C+TPC 21h, 3 crédits**

Technologies et Services Cloud - Cloud Computing, architectures, infrastructures, services, virtualisation- Traitement et stockage distribués - Programmation et Architectures applicatives - Systèmes d'agents et multi-agents – Agents intelligents - Architectures peer-to-peer - Travaux Pratiques.

#### **MTRS07S1. 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).

#### **MTRS08S1. Cybersécurité - C+TPC 24h, 3 crédits**

Introduction à la cybersécurité - Outils et processus de cybersécurité, administration système, vulnérabilités du système d'exploitation et de la base de données, types de cyberattaques. Analyse de risque en Cybersécurité. Recommandations techniques pour la cybersécurité.

#### **MTRS09S1. Réseaux sans fil - C+TPC 18h, 3 crédits**

Classification des réseaux sans-fil. Les réseaux WLAN : architecture, versions, protocole MAC, QoS.

Les réseaux ad hoc : auto-configuration, routage proactif et réactif, couche MAC. Les réseaux véhiculaires : exigences et contraintes des systèmes de transport intelligent (ITS), communications V2I et V2V, applications, standards, QoS, modèles de mobilité. Les réseaux de capteurs : architecture des WSN, clustering et mécanisme de routage avec contrainte d'énergie, standards de communications à faible puissance (IEEE 802.15.4, BLE), 6LowPAN et ZigBee. Internet des Objets : Piliers de l'IoT, éléments de l'IoT, applications IoT, protocoles de communication : MQTT, CoAP, LoRaWAN.

**MTRS10S1. Machine Learning pour les réseaux et la Cybersécurité - C+TPC 21h, 3 crédits**

Machine Learning, méthodes d'analyse de données. Procédures pour les réseaux et la cybersécurité, analyse, ce que le ML peut apporter à la cybersécurité, détection des attaques, prévention, etc.

**MTRS01S2 Mémoire de stage C 0 h, TPC 300 h, 30 crédits**

Il constitue une initiation aux techniques de la recherche. C'est la synthèse d'un travail de recherche de six mois dans une entreprise, un centre de recherche ou un laboratoire.