Université de Bretagne Occidentale

Faculté des Sciences & Techniques

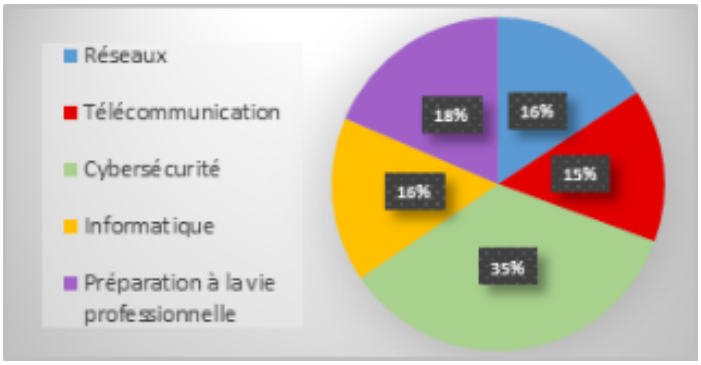
Master Réseaux et Télécommunications

Parcours Télécommunications, Réseaux et Cybersécurité

Objectifs

Le Master Télécommunications, Réseaux et Cybersécurité permet de former des diplômés ayant acquis les connaissances théoriques et les compétences pratiques pour s'insérer aisément dans les métiers de l'informatique, des télécommunications, des réseaux et de la cybersécurité.

Ce parcours est construit sur quatre disciplines fortement techniques que sont **les Télécommunications, les Réseaux, l'Informatique et la Cybersécurité** (voir Figure 1). Les disciplines enseignées se composent pour moitié d'enseignement théoriques et de spécialité et pour l'autre moitié d'enseignements pratiques (travaux pratiques, mini-projets et projets longs). Les diplômés sont ainsi à même de maîtriser les technologies actuelles et de demain dans chacune de ces disciplines. **Le master TRC est reconnu en tant que formation en cybersécurité** au niveau national.



Le Master Télécommunications, Réseaux et Cybersécurité fait preuve d'un partenariat fort avec les industriels locaux et régionaux. **La formation est ouverte à l'alternance** permettant ainsi une professionnalisation continue entre l'entreprise et les enseignements dispensés à l'université (par période de trois à quatre semaines).

Bien que particulièrement professionnalisante, la formation offre les fondamentaux pour une poursuite d'études en doctorat. Le stage de 6 mois se déroulant en fin de cursus peut donc être effectué indistinctement en laboratoire ou en entreprise.

DIPLÔME NATIONAL DE MASTER CONTRÔLÉ PAR L'ÉTAT

Compétences acquises

Le titulaire du Master Télécommunications et Réseaux est un professionnel qui pourra faire valoir des compétences techniques et pratiques dans les quatre domaines suivants :

Télécommunications :
• Choisir, adapter et optimiser des techniques de compression de données (voix, data et vidéo) et de codage correcteur d'erreurs
• Appréhender les normes de transmissions numériques et les technologies d'accès radio (2G, 3G, 4G et 5G)

Réseaux :
• Concevoir, dimensionner et administrer l'architecture et les protocoles réseaux
• Automatiser le déploiement et la configuration des réseaux grâce aux réseaux programmables et virtualisées
• Analyser et intégrer les solutions de Voix sur IP
• Maîtriser et mettre en œuvre les concepts de qualité de service (QoS)
• Superviser et appliquer un plan de continuité

Informatique :
• Gérer un projet en mode agile
• Concevoir des spécifications fonctionnelles et techniques
• Participer aux développements de projets conséquents

Cybersécurité :
• Concevoir et déployer une politique de sécurité
• Réaliser un cycle de vie sécurisé d'un développement logiciel
• Mettre en œuvre des stratégies de défense
• Réaliser des analyses de risque en suivant les normes IS0 2700X
• Détecter et réagir aux attaques
• Mettre en œuvre un plan de continuité d'activités

Conditions d'accès

Le Master s'adresse préférentiellement aux étudiants titulaires d'une licence du domaine des Réseaux et Télécommunications ou d'Informatique. Plus généralement, les étudiants ayant une licence du domaine de la formation "Sciences, Technologies, Santé" peuvent candidater.

L'accès à cette formation est également possible par le biais de la formation continue suivant les différents dispositifs de validation des acquis (VAE, VAPP 85 et VES).

Afin de garantir la qualité de la formation et la reconnaissance qu'elle a auprès du monde professionnel, **le Master Télécommunications, Réseaux et Cybersécurité est limité à 20 étudiants**. Les candidats sont choisis **sur dossier en fonction de leur qualité, de leur rigueur et de leur capacité de travail**.

Prérequis recommandés : Avoir des connaissances de base en réseaux et disposer d'un socle scientifique solide en électronique, mathématique et informatique.

Poursuite d'études

Ce parcours est indifférencié (recherche et professionnel) et est construit de sorte que les diplômés du Master Télécommunications, Réseaux et Cybersécurité puissent s'insérer directement dans le monde professionnel ou, pour ceux qui se destinent aux métiers de la recherche, poursuivre leurs études pour préparer un doctorat.

Par exemple, une partie des projets est orientée sur des problématiques d'entreprises du secteur, alors qu'une autre partie est orientée vers la recherche. Durant la totalité de son parcours, l'étudiant a ainsi l'occasion d'être confronté aux deux problématiques.

Chaque année, les différentes équipes de recherche du Laboratoire Lab-STICC UMR CNRS 6285 proposent des sujets de thèse financés et accessibles aux diplômés du Master.

Insertion professionnelle

Le diplômé du Master TRC est appelé à exercer principalement le métier d'ingénieur qui concourt à la mise en œuvre des Systèmes de Télécommunications et Réseaux et de la Cybersécurité. Les métiers occupés par les étudiants promus sont : Administrateur systèmes et réseaux, Architecte réseau, Audité de sécurité technique, Architecte sécurité, Analyste réponse aux incidents de sécurité, Ingénieur IP et Vidéo, Ingénieur en télécommunications, Ingénieur avant-vente, Chef de projet...

Le Master Télécommunications et Réseaux est une formation d'excellence. Les chiffres clefs (recensés en 2019) concernant l'insertion professionnelle (c'est-à-dire le 1er emploi après diplomation) sont :
• Insertion professionnelle : **100% des diplômés trouvent un travail 6 mois après l'obtention de leur diplôme**. Le **temps d'obtention médian d'un travail est de 0,75 mois** après diplomation.
• Revenu net mensuel : Le **revenu net mensuel médian est de 2300€**.
• Répartition géographique : **20% des diplômés trouvent un emploi en Bretagne**, 50% en Ile de France, et 30% dans une autre région.

Infos pratiques

Faculté des Sciences et Techniques à Brest
Ouvert en stage

Contacts

Responsable pédagogique
ESPES David

Contact administratif
Secrétariat du Département Electronique
secretariat-electronique@univ-brest.fr
Tel. 02 98 01 79 92

Université de Bretagne Occidentale

Faculté des Sciences & Techniques

Programme

M1

Semestre 7

Cryptographie et sécurité	44h
Cyber-protection des systèmes d'information	52h
Développement opérationnel (DevOps)	52h
Base de données, multi-tâches et programmation	44h
Processus et signaux aléatoires	44h
Préparation à la vie professionnelle	
- Communication	22h
- Anglais	22h
- Entreprise	10h

Semestre 8

Architectures réseaux virtualisées et programmables	50h
Introduction au traitement d'images	44h
Théorie de l'information et codage	44h
Bureau d'études / TAL	50h
Préparation à la vie professionnelle	
- Anglais	22h
- Communication	22h
- Entreprise	10h

M2

Semestre 9

Analyse de risque en sécurité	46h
Communications numériques et sécurisation de la couche physique	56h
Cyberdéfense des systèmes d'information	46h
Sécurité Logicielle	46h
Vidéo numérique, parole et protection des contenus multimédias	44h
Préparation à la vie professionnelle	
- Communication	22h
- Anglais	22h
- Entreprise	10h

Semestre 10

Gestion et mise en œuvre automatisée des politiques de sécurité	46h
Technique d'accès multiple : Furtivité des communications	32h
Bureau d'études	40h
Stage en entreprise ou laboratoire (4 à 6 mois)	620h

Dernière mise à jour le 02 mars 2026

Université de Bretagne Occidentale

Cryptographie et sécurité

Présentation

4 crédits ECTS

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 12h
Travaux Pratiques : 16h

La cryptographie est à la base de la sécurisation des transmissions. Connaître les principes de la cryptographie, les principaux algorithmes avec leurs forces et leurs faiblesses est indispensable au concepteur d'un système sécurisé.

Dans cette UE, nous donnons à l'étudiant une bonne connaissance des principes essentiels, une description des algorithmes importants, afin qu'il puisse choisir la méthode la plus adaptée à un contexte donné, en aillant une bonne compréhension de ses faiblesses potentielles.

Un accent particulier est également mis sur le chiffrement homomorphe qui permet de confier à un serveur un calcul complexe sans divulguer les données, et est donc par là-même appelé à connaître un essor important avec le développement du « cloud computing ».

Une sensibilisation à la vulnérabilité des principaux algorithmes actuels à une attaque par calculateur quantique terminera cet enseignement.

Objectifs

- Connaître les principes de la cryptographie et quelques algorithmes importants.
- Savoir choisir la méthode adaptée en fonction d'un cahier des charges.

Pré-requis nécessaires

Notions mathématiques : calcul modulaire, polynômes, vecteurs et matrices.

Compétences visées

- Algorithmes de chiffrement à clés secrètes et à clés publiques.
- Etude détaillée d'algorithmes: RC4, AES, RSA Fonctions de hachage.
- Signature cryptographique. Authentification.
- Déléguer un calcul sans divulguer ses données : chiffrement homomorphe.
- Distribution quantique des clés : exemple du réseau Chinois QUESS.
- Cryptosystèmes basés sur les codes correcteurs d'erreurs et sensibilisation à la cryptographie post-quantique (résistance à un attaquant disposant d'un calculateur quantique).

Bibliographie

Des références actualisées chaque année seront fournies en cours.

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CC	Ecrit et/ou Oral		67%	
UE	CC	Travaux Pratiques		33%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Oral	10	100%	

Université de Bretagne Occidentale

Cyber-protection des systèmes d'information

Présentation

6 crédits ECTS

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 16h
Travaux Pratiques : 20h

La cyber-protection nécessite en la conception d'une architecture réseau sécurisée. C'est la première barrière de défense d'une entité qui consiste à réduire au maximum sa surface d'attaque. Bien que différentes stratégies de protection existent, la stratégie de défense en profondeur est aujourd'hui la plus pragmatique. Cependant l'application d'une telle stratégie nécessite de connaître quelles contre-mesures peuvent faire face à un ou plusieurs types de menaces, savoir comment les déployer et les configurer et enfin pouvoir être en capacité de les maintenir dans le temps.

Cet enseignement se focalise sur la conception d'une architecture complexe qui repose sur le principe de la défense en profondeur. Deux concepts sont principalement abordés :

> Segmenter le réseau : la segmentation d'un réseau est probablement un des concepts les plus importants pour pouvoir réduire la surface d'attaque. Une méthodologie est présentée afin de pouvoir segmenter de manière optimale un système d'information tout en tenant compte de diverses contraintes opérationnelles et techniques.
> Réaliser la ségrégation entre zones : la ségrégation consiste à fournir des communications sécurisées entre zones segmentées d'un système. Cet enseignement propose des concepts pour sélectionner efficacement les mécanismes de sécurité et garantir leur bonne configuration.

La mise en place de la défense en profondeur est autant recommandée pour les systèmes d'information des technologies de l'information que pour ceux des technologies d'opération. Les spécificités de chacune de ces systèmes sont également abordées et les méthodologies adaptées au contexte d'application.

Pré-requis nécessaires

Bonne connaissance des réseaux, Bonne connaissance des systèmes d'opération

Compétences visées

> Pouvoir segmenter un réseau efficacement
> Assurer la ségrégation entre diverses zones d'un système d'information
> Savoir positionner les mécanismes de sécurité aux bons endroits et en minimiser le nombre
> Configurer les équipements de sécurité et les maintenir dans le temps
> Ecrire une politique de sécurité

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Université de Bretagne Occidentale

Développement opérationnel (DevOps)

Présentation

6 crédits ECTS

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 16h
Travaux Pratiques : 20h

Contrairement au cycle de vie du logiciel historique, le Développement opérationnel permet un développement et une intégration continue des fonctionnalités d'un système. Les avantages sont nombreux puisqu'il offre une plus grande flexibilité aux clients qui peuvent ajuster leur besoin en fonction de l'avancement du projet. De même pour le concepteur de l'application ou son développeur, l'automatisation du processus de déploiement offre une meilleure qualité de code en permettant de tester ou de valider le code de manière unitaire mais également lors de son intégration.

Le cycle de vie du développement opérationnel se base fortement sur le cycle de vie du logiciel historique tout en ajoutant des étapes pour gérer le déploiement de l'architecture. Nous étudierons dans cet enseignement l'intégralité du cycle de vie du DevOps que ce soit les étapes de planification, d'implémentation, de construction, de test qui représentent la partie développement et les étapes opérationnelles qui sont la publication, le déploiement, l'opération et la supervision de l'application.

La partie développement sera intégralement réalisée en utilisant les outils classiques comme le langage UML, le langage Java, Maven et la réalisation de tests unitaires avec JUnit. La partie opérationnelle se basera fortement sur les technologies de virtualisation et permettra d'acquérir les compétences pour publier un programme avec Gitlab, pour déployer ce dernier dans une architecture de pré-production en utilisant les containeurs et Kubernetes, la gestion des bugs avec Jenkins et la supervision de l'application avec Nagios.

Pré-requis nécessaires

Bonnes connaissances de la programmation java, bonnes connaissances de l'ingénierie logicielle, bonnes connaissances des réseaux

Compétences visées

- Pouvoir modéliser une application complexe
- Assurer l'intégration et le développement continues d'un projet informatique
- Maîtriser les technologies de virtualisation

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Université de Bretagne Occidentale

Base de données, multi-tâches et programmation

Présentation

Cette UE se déroulera sous la forme de cours, TD et TP (mini-projet).

Il y a 2 parties : les applications bases de données et les systèmes multi-tâches.

4 crédits ECTS

Volume horaire

Cours Magistral : 10h
Travaux Dirigés : 6h
Travaux Pratiques : 28h

Objectifs

> Savoir concevoir une base de données de type relationnel.
> Savoir exploiter la base via les requêtes SQL et le développement d'application WEB.
> Comprendre les problématiques temps réel, acquérir les bases de la programmation parallèle

Compétences visées

Bases de données :

> Etre en mesure d'effectuer une analyse informationnelle pertinente à partir d'un cahier des charges.
> Savoir effectuer une migration de données existantes dans une base de données relationnelle.
> Maitriser la modélisation Entités/Association.
> Savoir concevoir une base de données de type relationnelle : 1) MCD : Modèle Conceptuel de Données (Entités, Associations, Cardinalités) 2) MLD : Modèle Logique de Données (Tables, Colonnes, clés primaires et étrangères) 3) MPD : Modèle Physique de Données (implémentation dans un SGBD, implémentation graphique avec par ex. phpmyadmin)
> Savoir utiliser le langage SQL et développer une application WEB/PHP pour exploitation de la base de donnée.

Multi-tâches :

> Appréhender les problématiques temps réel et multitâche
> Comprendre les problématiques associées à la programmation multitâche/parallèle (synchronisation, concurrence, ressource critique)
> Connaitre et utiliser les outils permettant de gérer ces problématiques typiques (sémaphores)
> Maitriser un environnement de développement Temps Réel Multitâche (Windriver VxWorks)

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	90	42%	BDD (Bases de Données)
UE	CC	Travaux Pratiques		18%	BDD (Bases de Données)
UE	CC	Travaux Pratiques		40%	MT (Multi-Tâches)

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	90	60%	BDD (Bases de Données)
UE	Contrôle ponctuel	Oral	20	40%	MT (Multi-Tâches)

Université de Bretagne Occidentale

Processus et signaux aléatoires

Présentation

4 crédits ECTS

Volume horaire

Cours Magistral : 22h
Travaux Dirigés : 22h

Le modèle de signal déterministe ne suffit pas pour décrire les signaux naturels (la parole, signaux audio, biologiques, électrocardiogramme etc..) qui sont, par nature, aléatoires. La caractérisation des signaux aléatoires permet d'extraire des paramètres caractéristiques en vue de l'analyse et l'interprétation. La connaissance de ces caractéristiques est primordiale en vue de l'extraction d'un signal d'intérêt noyé dans le bruit ou en vue la dissimulation intensionnelle d'un signal d'intérêt dans du bruit. La maîtrise des outils pour mesurer les interactions entre signaux, permet de les quantifier afin de les atténuer (éviter). D'autres applications consistent à générer des signaux pour créer des interférences en vue du brouillage d'un signal cible.

Objectifs

> Analyser et caractériser les signaux aléatoires en vue de leur exploitation pour des applications en situations réelles (transmission de signaux, détection sonar, Radar, détection d'intrusion, médecine, etc...).
> Maîtriser le filtrage des signaux aléatoires (discrets et continus).
> Extraction de périodicités cachées dans un signal intercepté.
> Détection d'un signal noyé dans du bruit.
> La maîtrise du calcul des inter-corrélations entre les signaux pour éviter les interférences entre les signaux mais aussi pour générer le brouillage.
> Comprendre et implémenter des outils qui permettent de réduire les interférences entre les signaux
> Mesurer les inter-corrélations entre les signaux afin de mettre en évidence les interférences entre eux à éviter, ou en vue de générer des signaux pour le brouillage.

Pré-requis nécessaires

Probabilités et variables aléatoires ; Théorie du signal déterministe. Filtrage linéaire à temps continu et à temps discret.

Compétences visées

> Appréhender les outils de caractérisation des signaux aléatoires
> Savoir mesurer et quantifier l'indépendance entre les signaux (fonctions de covariance, corrélation, etc..).
> Analyse spectrale des processus et signaux aléatoires stationnaires au second ordre (PASSO). (Périodogramme, Densité spectrales de puissance).
> Appréhender les outils d'extraction d'un signal d'intérêt dans un mélange de signaux.
> Bruit blanc, bruit Gaussien, signaux cyclo-stationnaires.

Bibliographie

[1] - A. Mansour, A. Quinquis, E. Radoi, Signaux et systèmes : Signaux, filtrage et décision, ISBN 978-2746248595, Lavoisier Hermès Science Publications, Paris, 2019.

[2] - G. Jourdain, Cours de traitement du signal, Institut Polytechnique de Grenoble, 2009.

[3] - Francis Cottet, Traitement des signaux et acquisition de données : cours et exercices corrigés, Paris : Dunod, 2009.

[4] - André Quinquis, Emanuel Radoi, et al., Le traitement du signal sous Matlab® : pratique et applications, Paris : Hermès science publications : Lavoisier, 2007.

[5] - Messaoud Benidir, Théorie et traitement du signal. 2, Méthodes de base pour l'analyse et le traitement du signal : Cours et exercices corrigés, Paris : Dunod, 2004.

[6] - Alain Yger, Théorie et analyse du signal : cours et initiation pratique via MATLAB et SCILAB, Paris : Ellipses, 1999.

[7] - Robert Dalmasso, Patrick Witomski, Analyse de Fourier et applications : exercices corrigés, Paris, Masson, 1996.

[8] - Gilbert Demengel, Paul Bénichou, Rosine Bénichou, Distributions et applications : séries de Fourier, transformations de Fourier et de Laplace : outils pour l'ingénieur, Paris : Ellipses, 1996.

[9] - Paul Bénichou, Rosine Bénichou, Norbert Boy, Séries de Fourier, transformation de Laplace, Paris : Ellipses, 1995. D'autres références, actualisées chaque année, seront fournies en cours

Modalités de contrôle des connaissances

Université de Bretagne Occidentale

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Université de Bretagne Occidentale

Préparation à la vie professionnelle

6 crédits ECTS

Université de Bretagne Occidentale

Communication

Présentation

L'UE communication est destinée aux étudiants de master au semestre 7.

2 crédits ECTS

Volume horaire

Cours Magistral : 7h
Travaux Dirigés : 15h

Objectifs

L'objectif est de maîtriser une culture scientifique de spécialité, d'initier une réflexion sur l'épistémologie et l'histoire des sciences et de savoir communiquer sur ses travaux de recherche en les vulgarisant.

Un autre objectif est celui de l'insertion professionnelle par le biais de la rédaction d'une fiche de poste dans leur spécialité et la sélection de candidats aptes à y répondre.

Compétences visées

Les étudiants développent leurs capacités rédactionnelles par la rédaction d'un article scientifique ou de médiation scientifique.

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CC	Ecrit et/ou Oral		1/1	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	Contrôle ponctuel	Oral	15	1/1	

Université de Bretagne Occidentale

Anglais

Objectifs

Intégration dans le monde du travail.

3 crédits ECTS

Volume horaire

Cours Magistral : 8h
Travaux Dirigés : 14h

Compétences visées

Préparer une candidature à l'embauche / Comprendre l'organisation d'une entreprise / Participer et animer une réunion / Prendre des notes / Rédiger un compte-rendu

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CT	Ecrit - devoir surveillé	90	1/2	
EC	CC	Ecrit et/ou Oral		1/2	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CT	Ecrit - devoir surveillé	30	1/1	

Université de Bretagne Occidentale

Entreprise

1 crédits ECTS

Volume horaire

Autres : 10h

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
Autres	Autre modalité	Ecrit et/ou Oral		1/1	validation par "badge" - Pas de session 2 -

Université de Bretagne Occidentale

Architectures réseaux virtualisées et programmables

Présentation

6 crédits ECTS

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 16h
Travaux Pratiques : 18h

L'architecture réseau IP conventionnelle manque de flexibilité et est complexe à faire évoluer. L'automatisation de la configuration du réseau et son optimisation en termes d'ingénierie réseau requiert généralement une vue globale de ce dernier. Il est nécessaire d'utiliser un nouveau paradigme pour cela. Les réseaux programmables SDN répondent à ces besoins en dissociant le plan de données qui permettra uniquement de gérer la commutation des messages du plan de contrôle qui sera l'intelligence du réseau. Le plan de management permet de communiquer les actions à réaliser au plan de contrôle.

Dans cet enseignement, les spécificités de l'architecture SDN sera étudiée. Un focus sur sa cybersécurité sera réalisé. De par la centralisation de la connaissance de l'architecture, de nombreuses optimisations peuvent être apportées aux protocoles actuels. La conception d'application optimisée sera le cœur d'un tel enseignement. Cette conception mettra en avant l'utilité d'exploiter plusieurs tables de commutation au sein du plan de données, et que de nombreuses optimisations peuvent être réalisées par ce biais.

Pré-requis nécessaires

Bonnes connaissances des réseaux, bonnes connaissances sur les mécanismes de cyber-protection, bonnes connaissances de la programmation java, bonnes connaissances de l'ingénierie logicielle

Compétences visées

> Pouvoir déployer de manière sécurisé un réseau virtualisé et programmable
> Savoir concevoir une fonction réseau virtualisée
> Savoir optimiser le fonctionnement des protocoles réseaux de l'architecture conventionnelle en utilisant les spécificités de centralisation et de programmation des réseaux programmables
> Pouvoir permettre le passage à l'échelle des réseaux programmables

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Université de Bretagne Occidentale

Introduction au traitement d'images

Présentation

Outils de base du traitement et de la protection des images, illustrés par de nombreux exemples d'applications : représentation de la couleur, filtrage bidimensionnel appliqué à la réduction du bruit et à la restauration d'images floues, compression appliquée à la réduction du volume mémoire occupé par une photographie numérique, reconnaissance de l'écriture, sécurisation d'une photo par tatouage.

6 crédits ECTS

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 8h
Travaux Pratiques : 20h

Objectifs

Acquérir une vision d'ensemble du domaine du traitement et de la protection des images, à travers des applications variées. Les détails mathématiques trop complexes sont volontairement évités, au profit de l'explication de la démarche à adopter face à un problème de traitement d'images.

Pré-requis nécessaires

Connaissances de base en mathématiques, notamment les notions de matrice et de vecteur, et en traitement du signal (filtrage numérique). Programmation en Matlab.

Compétences visées

- Images numériques, formats d'images, représentation de la couleur.
- Compression d'images: transformations linéaires, quantification vectorielle, JPEG
- Filtrage bidimensionnel. Application à la réduction de bruit et à la détection de contours.
- Restauration d'images floues et application à la correction des défauts d'acquisition (bougé, défocalisation).
- Introduction à la reconnaissance de formes: caractérisation et classification de chiffres manuscrits.
- Introduction à la notion de réseau de neurones, application à l'image.
- Sécurité : protection des images par tatouage.
- Tatouage détectable et indétectable.
- Résistance du tatouage aux attaques et aux transformations (compression, photocopie, ...).

Bibliographie

1. Gilles Burel, «Introduction au traitement d'images. Simulation sous Matlab », Hermès Sciences Publications
2. William K. Pratt, "Digital Image Processing", Wiley-Interscience publications
3. Des références bibliographiques actualisées chaque année seront données en cours.

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CC	Ecrit - devoir surveillé		67%	
UE	CC	Travaux Pratiques		33%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	90	100%	

Université de Bretagne Occidentale

Théorie de l'information et codage

Présentation

Les transmissions numériques reposent très largement sur la capacité à coder et décoder les données, afin d'une part de réduire les débits nécessaires (codage de source) et d'autre part de sécuriser l'intégrité des données (codage de canal). Cette UE présente les principes du codage, en l'illustrant par des exemples concrets. Les éléments de théorie de l'information nécessaires à la compréhension du codage sont également présentés.

6 crédits ECTS

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 12h
Travaux Pratiques : 16h

Objectifs

> Donner à l'étudiant une bonne maîtrise des techniques de codage/décodage qui sont à la base des normes de communications numériques récentes.
> Sensibiliser les étudiants aux avantages du numérique pour la sécurisation de l'intégrité des informations.

Pré-requis nécessaires

> Notions mathématiques de base : fonction logarithme, vecteurs et matrices.
> Probabilités.
> Eléments de calcul polynômial, notamment la division Euclidienne des polynômes.

Compétences visées

> Description sommaire d'une chaine de transmission : source, codeur de source, codeur de canal, émetteur, canal de transmission.
> Théorie de l'information : mesure de l'information, entropie, entropie conditionnelle, entropie conjointe, propriétés des entropies, relations entre les entropies, mesure de l'information transmise sur un canal, capacité du canal, adaptation d'une source au canal.
> Codage de source : Introduction, classification des codes, code à longueur fixe, code à longueur variable, code sans préfixe, code instantané, code non séparable, inégalité de Kraft/Mc Millan, limite inférieure de la longueur moyenne d'un code, longueur moyenne d'un code, longueur moyenne minimale d'un code, premier théorème de Shannon : démonstration, extension de source, entropie des sources étendues, notion d'efficacité et de redondance, procédure de construction des codes, procédure de Shannon-Fano, procédure de Huffman, procédure de Shannon-Fano et d'Huffman.
> Codage de canal : classification des codes, principe des codes en bloc linéaires (CBL), paramètres de performance, matrice génératrice et matrice de contrôle de parité, code dual, correction des erreurs basée sur le syndrome, capacité de détection et de correction d'erreurs d'un CBL, codes de Hamming et codes à longueur maximale, limite du rendement d'un CBL et lien avec la capacité du canal, probabilité d'erreur en sortie du décodeur de canal, codes cycliques, représentation polynomiale, polynôme générateur et matrice génératrice d'un code cyclique, construction des codes cycliques, décodage des codes cycliques, codes de Golay et BCH.

Bibliographie

1. A. Spataru, Fondement de la théorie de la transmission de l'information (Presses polytechniques et universitaires romandes).
2. M. Joindot et A. Glavieux, Communications numériques (Masson).

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CC	Ecrit - devoir surveillé		67%	
UE	CC	Travaux Pratiques		33%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	90	100%	

Université de Bretagne Occidentale

Bureau d'études / TAL

Présentation

6 crédits ECTS

Volume horaire

Projet tutoré : 50h

Cette unité d'enseignements consiste en la réalisation d'un projet long de 6 mois. Les étudiants sont répartis par groupe de 4 et reçoivent un cahier des charges composés de 4 lots. Chaque groupe possède un projet différent qui nécessite de coder une application SDN liée à un protocole réseau connu.

Ce projet permet de mettre en pratique les compétences acquises durant l'UE de DevOps sur la conception d'un projet informatique conséquent, et sur son déploiement en intégration continue et durant l'UE Réseaux programmables en concevant une fonction réseau virtualisée complexe qui représente l'optimisation d'une fonctionnalité réseau de l'architecture conventionnelle (ex : découverte automatique de la topologie et du voisinage, gestion centralisée des VLANs avec mise en place automatique des trunks et des liens d'accès, réalisation d'un pare-feu à états...).

Pré-requis nécessaires

Bonnes connaissances des réseaux, bonnes connaissances sur les mécanismes de cyber-protection, bonnes connaissances de la programmation java, bonnes connaissances de l'ingénierie logicielle

Compétences visées

- Pouvoir répondre à un cahier des charges
- Gérer un projet et fournir à temps divers livrables
- Pouvoir concevoir une application SDN et la déployer automatiquement

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
	CC	Autre nature		100%	

Université de Bretagne Occidentale

Préparation à la vie professionnelle

6 crédits ECTS

Université de Bretagne Occidentale

Anglais

Objectifs

Intégration dans le monde du travail.

3 crédits ECTS

Volume horaire

Cours Magistral : 8h
Travaux Dirigés : 14h

Compétences visées

Présenter des résultats et argumenter / Conseiller / Simplifier / Vulgariser / Rédiger une note de synthèse / Présentation orale d'un objet technique ou d'une campagne d'information

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CT	Ecrit - devoir surveillé	90	1/2	
EC	CC	Autre nature		1/2	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CT	Oral	10		

Université de Bretagne Occidentale

Communication

Présentation

L'UE communication est destinée aux étudiants de master au semestre 8.

2 crédits ECTS

Volume horaire

Travaux Dirigés : 15h
Cours Magistral : 7h

Objectifs

L'objectif est de développer une analyse critique des médias par l'étude du monde de l'édition scientifique et de la presse généraliste et de spécialité.

Compétences visées

Les étudiants sont amenés à développer leurs capacités rédactionnelles à travers la réalisation d'une revue de presse puis d'un dossier de presse mais également d'expression orale par la conception de podcasts.

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CC	Ecrit et/ou Oral		1/1	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CT	Oral	15	1/1	

Université de Bretagne Occidentale

Entreprise

1 crédits ECTS

Volume horaire

Travaux Dirigés : 10h

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CC	Autre nature		1	Pas de session 2

Université de Bretagne Occidentale

Analyse de risque en sécurité

Présentation

5 crédits ECTS

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 14h
Travaux Pratiques : 16h

L'analyse de risque en cybersécurité est aujourd'hui incontournable pour réaliser un système de gestion pour la sécurité de l'information.

Elle permet d'identifier les risques de sécurité qu'encourt un système et les contremesures nécessaires pour atteindre un niveau de risque acceptable.

Ce module aborde de manière concrète les standards ISO 27000, ISO 27001 et ISO 27005.

Objectifs

Ce module permet de présenter les concepts clefs pour réaliser une analyse de risque en cybersécurité sur une architecture hétérogène et complexe.

Pré-requis nécessaires

Module Cyber-protection d'un système d'information au M1 TRC : Connaissance des mesures de sécurité énoncées dans l'ISO 27002

Compétences visées

Les compétences visées sont les suivantes :

- Pouvoir respecter les exigences nécessaires à la conception d'un système de gestion pour la sécurité de l'information
- Pouvoir évaluer les risques en cybersécurité sur un système
- Etre capable de choisir les contremesures adaptées pour atteindre un niveau de risque acceptable

Descriptif

Le module est composé pour moitié d'enseignements théoriques :

- Identification des biens principaux et de support d'un système
- Etablir les critères d'évaluation des risques et des impacts
- Identification des menaces sur le système
- Identification des vulnérabilités d'un système
- Identification de l'impact sur un système d'un incident de cybersécurité
- Evaluation et acceptation du risque

et pour moitié d'enseignements pratiques :

- Application de l'ISO 27005 sur un système complexe
- Audit d'un système

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Université de Bretagne Occidentale

Communications numériques et sécurisation de la couche physique

Présentation

La plupart des standards actuels de télécommunications utilisent la technologie multi-porteuses de type OFDM et ses dérivées.

Cette UE permet d'appréhender finement cette technologie.

Un accent particulier est également mis sur la sécurisation du canal de transmission entre deux utilisateurs légitimes.

5 crédits ECTS

Volume horaire

Cours Magistral : 20h
Travaux Dirigés : 16h
Travaux Pratiques : 20h

Objectifs

Comprendre les défis et les enjeux de la couche PHY dans les systèmes de communications numériques.

Compétences visées

> Étude des paramètres fondamentaux d'une chaîne de communications numériques (débits, filtrage de Nyquist, bande/efficacité spectrale, modulations linéaires, PAPR, capacité canal, SNR, BER, bilan de liaison et sensibilité du récepteur).
> Étude de la couche PHY des systèmes multi-porteuses de type OFDM à travers les standards actuels.
> Introduction à la sécurisation de la couche PHY (techniques de codage, génération de clé à partir des caractéristiques du canal radio des utilisateurs légitimes).

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	90	60%	
UE	CC	Travaux Pratiques		40%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	90	100%	

Université de Bretagne Occidentale

Cyberdéfense des systèmes d'information

5 crédits ECTS

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 14h
Travaux Pratiques : 16h

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Université de Bretagne Occidentale

Sécurité Logicielle

4 crédits ECTS

Volume horaire

Cours Magistral : 14h
Travaux Dirigés : 12h
Travaux Pratiques : 20h

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Université de Bretagne Occidentale

Vidéo numérique, parole et protection des contenus multimédias

Présentation

5 crédits ECTS

Volume horaire

Cours Magistral : 12h
Travaux Dirigés : 8h
Travaux Pratiques : 24h

Avec les progrès en matière de transmission et de stockage en ligne, la quantité de contenus digitaux tels que la parole et la vidéo sur internet a explosé et continue d'augmenter. Cela a conduit au développement d'un grand nombre d'algorithmes de plus en plus sophistiqués afin de réduire le débit de transmission et la quantité d'information à stocker ainsi que de protéger les données.

Ce cours s'intéresse aux principaux flux de données que sont les signaux audio et la vidéo numérique qui circulent sur le réseau. La compression de la vidéo numérique ainsi que les méthodes de codage à très bas débit du signal audio sont décrites. La protection de ces données numériques contre les altérations volontaires ou la copie revêt des enjeux importants. Des techniques permettant d'identifier la source des données et de détecter une éventuelle modification sont également abordées dans cette UE ainsi que la robustesse de ces méthodes par rapport à différent types d'attaques.

Les notions étudiées en cours sont implémentées par des simulations réalistes au cours des mini-projets.

Objectifs

> Comprendre le codage à très bas débit de la parole en vue de sa transmission dans les réseaux informatiques et aussi pour la protection des contenus.
> Comprendre et paramétrer un compresseur vidéo.
> Comprendre les méthodes fondamentales pour la protection des contenus multimédia.

Pré-requis nécessaires

Calcul matriciel, Transformée en Z, Transformée de Fourier ; Communications numériques ; Processus et signaux aléatoires ; Codage de source, compression JPEG ; Traitement d'images.

Compétences visées

> Identifier et exploiter les technologies utilisées dans les codecs.
> Quantification logarithmique et application au codeurs de la forme d'onde (codec G7XX).
> Modélisation par prédiction linéaire et application à l'extraction des pitchs et des formants de la parole.
> Conception des vocodeurs paramétriques à bas débit (FS1015, LPCXX) et des codeurs hybrides.
> Notion de cryptage du signal audio.
> Compression et transmission de séquences d'images (MPEG). Compensation de mouvement.
> Prédiction causale et anti-causale. Régulation de débit.
> Notion de codage arithmétique. Détection et caractérisation d'objets.
> Sécurité, protection: tatouage numérique des vidéos.
> Techniques temporelles, notamment par perturbation des vecteurs de mouvement, pour l'embrouillage ou le marquage des vidéos.
> Robustesse du tatouage vidéo par rapport à différents types d'attaque, par recompression, par filtrage, par permutations d'images.
> Aspects psycho-visuels : invisibilité de la protection insérée dans le flux vidéo et compromis invisibilité/robustesse.

Bibliographie

Des références actualisées chaque année seront fournies en cours

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	60%	
UE	CC	Travaux Pratiques		40%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120		

Université de Bretagne Occidentale

Préparation à la vie professionnelle

6 crédits ECTS

Université de Bretagne Occidentale

Communication

Présentation

Deux programmes distincts en fonction du choix de la voie orientée professionnalisante ou recherche.

2 crédits ECTS

Volume horaire

Travaux Dirigés : 15h
Cours Magistral : 7h

Objectifs

Master professionnel

L'objectif est de cibler le marché du travail afin d'affiner son projet professionnel pour trouver l'offre de stage de fin d'études la plus adaptée au cursus et aux objectifs de carrière. Les étudiants sont amenés à se créer un réseau professionnel, à valoriser leur profil universitaire afin de postuler auprès des entreprises.

Master recherche

L'objectif est d'acquérir une connaissance de soi, des métiers et de l'environnement de la recherche, des débouchés du master, du doctorat ou post-doctorat afin de candidater efficacement, de construire son insertion professionnelle ou sa poursuite d'études dans un contexte concurrentiel.

Compétences visées

Master professionnel

Les étudiants sont amenés à se créer un réseau professionnel, à valoriser leur profil universitaire afin de postuler auprès des entreprises. Ils affinent leurs compétences à l'oral pour maîtriser leur entretien de recrutement. Ils développent également leurs compétences rédactionnelles par une préparation à l'élaboration du rapport de stage. Des notions de management et de gestion de projet leur sont dispensées afin qu'ils puissent s'insérer rapidement dans leur équipe professionnelle.

Master recherche

Les étudiants sont amenés à construire leur projet de doctorat et à appréhender la méthodologie de la thèse par l'utilisation d'outils de recherche et de communication. Ils travaillent à organiser une réflexion personnelle objective à partir d'une recherche bibliographique et d'hypothèses scientifiques et développent leur esprit critique. Ce travail est complété par une réflexion sur la propriété intellectuelle, la fraude ou l'erreur scientifique, l'analyse des mécanismes de l'innovation, les enjeux des rapports entre scientifiques et société et l'éthique de la recherche dans un contexte compétitif. Les travaux comportent des exposés sur le monde de la recherche, la présentation d'un état de l'art en lien médiatisant leur sujet de stage de recherche et une présentation de leur projet professionnel.

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CC	Ecrit et/ou Oral		1/1	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
EC	CT	Oral	15	1/1	

Université de Bretagne Occidentale

Anglais

3 crédits ECTS

Volume horaire

Cours Magistral : 8h
Travaux Dirigés : 14h

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
	CC	Ecrit et/ou Oral		100	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
	CT	Oral	15	100	

Université de Bretagne Occidentale

Entreprise

1 crédits ECTS

Volume horaire

Autres : 10h

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
Autres	Autre modalité	Ecrit et/ou Oral		1/1	validation par "badge" - Pas de session 2 -

Université de Bretagne Occidentale

Gestion et mise en œuvre automatisée des politiques de sécurité

5 crédits ECTS

Volume horaire

Cours Magistral : 14h
Travaux Dirigés : 14h
Travaux Pratiques : 18h

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	120	100%	

Université de Bretagne Occidentale

Technique d'accès multiple : Furtivité des communications

Présentation

Les techniques d'accès multiple constituent un élément essentiel de beaucoup de normes récentes de communication numérique. Leur intérêt est encore renforcé par l'émergence de l'Internet des Objets. Cette UE aborde les différentes méthodes permettant l'accès multiple à un canal de transmission. Un accent particulier est également mis sur la discrétion de certaines de ces méthodes (furtivité), permettant par là de réduire les risques d'attaque et d'interception des communications.

3 crédits ECTS

Volume horaire

Cours Magistral : 12h
Travaux Dirigés : 8h
Travaux Pratiques : 12h

Objectifs

> Connaissance des principes de communication numérique avec accès multiple.
> Expérience concrète de la programmation et de l'évaluation d'un système de transmission à accès multiple.
> Savoir utiliser l'étalement de spectre pour protéger une transmission.
> Savoir évaluer la probabilité d'interception et la résistance au brouillage.

Pré-requis nécessaires

Communications numériques.

Compétences visées

> Etude des méthodes et techniques d'étalement de spectre (séquences directes, sauts de fréquence) et des méthodes d'accès multiples (TDMA, FDMA et CDMA).
> Codes de Gold, Kasami et OVSF (codes orthogonaux à longueur variable).
> Principe et performances des différents récepteurs. Synchronisation: acquisition et poursuite.
> Exemples de normes et systèmes basés sur l'accès multiple. Sécurité : évaluation de la discrétion (furtivité).
> Probabilité d'interception. Résistance au brouillage.

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CC	Ecrit - devoir surveillé		67%	
UE	CC	Travaux Pratiques		33%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CT	Ecrit - devoir surveillé	60	100%	

Université de Bretagne Occidentale

Bureau d'études

4 crédits ECTS

Volume horaire

Projet tutoré : 40h

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
	CC	Autre nature		100%	

Université de Bretagne Occidentale

Stage en entreprise ou laboratoire (4 à 6 mois)

Présentation

Découvrir le monde de l'entreprise. Mise en application des connaissances acquises.

18 crédits ECTS

Volume horaire

Stages : 620h

Objectifs

Un stage de longue durée en fin de 2ème année (4 à 6 mois à partir du mois de mars) permet de compléter les enseignements théoriques et pratiques dispensés lors des 2 années du master.

Ce stage s'effectue préférentiellement au sein d'une entreprise ou d'un laboratoire de recherche dont le secteur d'activités est lié aux enseignements dispensés. Il donne lieu à la rédaction d'un mémoire et à une soutenance devant un jury composé d'universitaires intervenant dans le Master et des professionnels de l'entreprise ou du laboratoire concerné. Un membre de l'équipe pédagogique fait office de tuteur. Il est chargé des relations avec l'étudiant et l'entreprise ou le laboratoire.

Ce stage peut également être effectué à l'étranger.

Pré-requis nécessaires

Avoir suivi les enseignements du S9 et S10.

Compétences visées

> Mettre en pratique les connaissances acquises durant la formation à l'université et acquérir de nouvelles compétences dans le milieu professionnel.
> Participer à la production des biens et services pour le marché.
> Faire preuve d'autonomie et de capacités d'adaptation.
> Développer son employabilité sur le marché du travail.
> Le stage est régi par une convention de stage signée par le stagiaire, l'entreprise et l'université.
> En entreprise, le stagiaire est suivi par un maître de stage et il est représenté à l'université par un tuteur universitaire.

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
Stages	CC	Travaux Pratiques		33%	Le CC correspond à l'évaluation du travail de stage par l'encadrant (d'entreprise ou de laboratoire)
Stages	CT	Ecrit - rapport		33%	
Stages	CT	Oral - soutenance	40	34%	

Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
Stages	Report de notes	Autre nature			