FICHE D'UNITÉ D'ENSEIGNEMENT

1. Données concernant le programme d'études

1.1	Établissement d'enseignement supérieur	Université Technique de Cluj-Napoca
1.2	Faculté	Électronique, Télécommunications et Technologie de l'Information
1.3	Département	Télécommunications
1.4	Domaine d'étude	Ingénierie Électronique, Télécommunications et Technologies de l'Information
1.5	Cycle d'études universitaires	Master
1.6	Intitulé du programme d'études /de la qualification	Traitement du signal et des images (en français)
1.7	Type de formation	FP – formation présentielle
1.8	Code de l'UE	17.00

2. Données concernant l'UE

2.1	Intitulé					Techniques de cryptage et tatouage					
2.2	Domaine d'études (subject area)					Ingénierie électronique et télécommunications					
2.3	Responsable de l'UE					Monica Borda, Professeur des universités					
2.4	Responsable applications (TDs et TPs)					Raul Malutan, Maître de conférences					
2.5	Année d'études	II	2.6	Semestre	3	2.7	Méthode d'évaluation	E	2.8	Régime de l'UE	DA/DI

3. Volume horaire estimée

3.1	Nombre d'heures par semaine	3	3.2	dont cours	2	3.3	applications	1
3.4	Nombre total d'heures dans le plan d'enseignement	42	3.5	dont cours	28	3.6	applications	14

Distribution du temps	Heures
Étude individuelle	14
Étude en utilisant le support et les notes de cours, manuels de spécialité et références bibliographiques	14
Documentation supplémentaire en bibliothèque, en utilisant des plateformes électroniques ou sur le terrain.	-
Préparation TDs/TPs, devoirs, rapports, projets, portefeuilles, essais	28
Tutorat	2
Evaluation	2
Autres activités	-

3.7	Nombre total d'heures étude individuelle	58
3.8	Nombre total d'heures par semestre	100
3.9	Nombre de crédits ECTS	4

4. Pré-requis : (le cas échéant)

4.1	De curriculum	-
4.2	En compétences	Connaissance des mathématiques, de la théorie de l'information, du traitement du signal, des circuits analogiques et numériques, de la programmation

5. Conditions (le cas échéant)

5.1	De déroulement du cours	Cluj-Napoca,
5.2	De déroulement des applications	Cluj-Napoca,

6. Compétences spécifiques

Compétences professionnelles	**C2 Application de méthodes de base pour l'acquisition et le traitement des signaux** C2.1 Caractérisation temporelle, spectrale et statistique des signaux C2.3 Utilisation de supports de simulation pour l'analyse et le traitement des signaux C2.4 Utilisation de méthodes et d'outils spécifiques pour l'analyse des signaux C2.5 Conception de blocs fonctionnels élémentaires de traitement du signal numérique avec déploiement de matériel et de logiciels **C4 Conception, mise en œuvre et exploitation de services de données, voix, vidéo, multimédia, basé sur compréhension et application des notions fondamentales de dans le domaine des communications et de la transmission de l'information** C4.2 Résoudre des problèmes pratiques en utilisant une connaissance générale des techniques multimédias
Compétences transversales	**CT.3 Adaptation aux nouvelles technologies, développement professionnel et personnel par la formation continue à l'aide de sources de documentation imprimées, de logiciels spécialisés et de ressources électroniques en roumain et, au moins, dans une langue internationale de circulation internationale (français)**

7. Objectifs d'apprentissage de l'UE (ressortant de la grille des compétences spécifiques)

7.1	Objectif général	Développement de compétences dans le domaine des systèmes cryptographiques
7.2	Objectifs spécifiques	1. L'assimilation des connaissances théoriques concernant les technologies cryptographiques de base 2. Assimilation des connaissances théoriques concernant les attaques et les modèles de sécurité dans les systèmes informatiques 3. Acquérir les compétences nécessaires pour développer des applications logicielles et des systèmes matériels dans le domaine de la cryptographie, du marquage de transparence des données et du cryptage d'images

8. Contenu

8.1. Cours (syllabus)		Méthodes d'enseignement	Remarques
1	Bibliographie. Objectives du cours. Nécessité de la sécurité.Organisation du cours. 1. Introduction. 1.1 Terminologie. 1.2 Courte histoire. 1.3 Cryptosystèmes . 1.4 Attaques et modèles de sécurité	Enseignement direct, discussion	Vidéo projecteur et tableau blanc interactif
2	2. Fondements mathématiques en cryptographie		
3	3.Cryptographie conventionnelle (symétrique).3.1 Cryptographie classique (Caesar, Polybius, Trithemius, Playfair, Vigénère)		
4	3.2 Cryptographie symétrique moderne. 3.2.1 Algorithmes de chiffrement par blocs(principes, Feistel, DES,AES,T-DES,IDEA, etc., types et modes d'algorithmes). 3.2.2 Générateurs de suites aléatoires et chiffrement en continu		

5	3.3 Confidentialité avec cryptographie classique. 3.3.1 Chiffrement des canaux de communication. 3.3.2 Chiffrement des données pour stockage. 3.3.3 Gestion des clefs dans la cryptographie symétrique. 3.3.4 Protocoles élémentaires pour la cryptographie symétrique		
6	4. Cryptographie à clef publique (cryptographie asymétrique). 4.1 Principe et taches. 4.2 Algorithmes à clef publique(RSA, Diffie-Hellman, cryptosystèmes a courbes elliptiques)		
7	4.3 Authentification		
8	4.4Signatures numériques. 4.5Protocoles pour signatures numériques. 4.6Gestion des clefs dans la cryptographie a clef publique		
9	5. Tatouage (digital watermarking)		
10	6. Cryptographie ADN		
11	7. Cloud computing		
12	8. Politiques de sécurité		
13	9. Autres applications de sécurité(KERBEROS, PEM, MSP, PGP, PKCS)		
14	Récapitulation envisageant l'examen		
8.3. Applications (TPs)		Méthodes d'enseignement	Remarques
1	Introduction à Matlab	L'expérience didactique, la simulation, le travail d'équipe	
2	Cryptographie classique		
3	Algorithmes symétriques		
4	Cryptographie avec clés publiques		
5	Marquage transparent		
6	Cryptage d'image		
7	Cryptage ADN. Certificats numériques		

Références bibliographiques :
1. Titu Băjenescu, Monica Borda- *Securitatea în informatică şi telecomunicaţii*- Ed. Dacia 2001
2. M. Borda, *Fundamentals in Information Theory and Coding* – Springer 2011
3. Bruce Schneier - *Applied Cryptography – Protocols, Algorithms and Source Code in C*. Second Edition- John Willey & Sons, 1996
4. W. Stallings – *Cryptography and network security. Principles and practice*- Prentice-Hall, 2nd edition, 1999
5. A.J. Menezes,P.von Oorschot,S.A. Vanstone- *Handbook of Applied Cryptography* - CRC Press, 1997
6. Cox, J. Bloom, M. Miller-*Digital Watermarking: Principles & Practice* - Morgan Kaufmann Publishers, 2001
7. Bruce Schneier, *Cryptographie appliquee*, Vuibert, 2010, Paris
8. Niels Ferguson, Bruce Schneier, *Sécurité de l'information et des systèmes : Cryptographie : En pratique*, Vuibert 2004, Paris
9. Vic(J.R.) Winkler, *La securite dans le cloud* , Pearson, 2011, Paris

9. Corroboration du contenu de la discipline avec les attentes des représentants de la communauté, des associations professionnelles et des employeurs dans le domaine lié au programme

Les compétences acquises seront requises pour les collaborateurs qui développent leur activité dans le domaine du développement (programmation) et de l'utilisation des applications bio-informatiques.

10. Évaluation

10. Evaluation

Type d'activité	10.1 Critères d'évaluation	10.2 Méthode d'évaluation	10.3 Pourcentage de la note finale

10.4 Cours	Le niveau d'acquisition des connaissances théoriques et le niveau des compétences acquises	Réponse correcte à 20 questions de test de grille, chaque réponse correcte étant pondérée avec 0,3 et synthétisant 2 sujets théoriques, chaque sujet complètement présenté étant pondéré avec 1,5.	50%
10.5 TPs	Niveau de compétences acquises	Chaque étudiant choisira un thème de mini-projet. Le mini-projet doit contenir : - Une application douce - Un article scientifique (minimum 8 pages) - Une présentation MS Power-Point qui comprendra à la fois une description théorique du projet ainsi qu'une description de l'application et des résultats obtenus	50%

10.6 Normes minimales de performance

Niveau qualitatif

- Connaître le rôle d'un cryptosystème
- Connaître les protocoles pour les communications cryptographiques symétriques
- Connaître les protocoles de communications cryptographiques asymétriques et hybrides
- Connaître les protocoles pour les signatures numériques
- En savoir plus sur les protocoles d'échange de clés et les protocoles d'authentification
- Pour implémenter des algorithmes cryptographiques: algorithmes symétriques - standard de cryptage des données (DES)
- Pour implémenter des numéros de bloc (LUCIFER, IDEA, RC2, RC4, AES)
- Identifier les générateurs de séquences pseudo-aléatoires et leurs chiffres basés
- Connaître les fonctions de hachage unidirectionnelles
- Connaître les algorithmes à clés publiques (principes, algorithmes de sac à dos, RSA, LUC)
- Connaître l'algorithme de clé numérique (DSA);
- Connaître les techniques cryptographiques: longueur et gestion des clés

Pour utiliser diverses applications: filigrane transparent, cryptage d'image

Niveau quantifatif

- ✓ Réponse correcte à 10 questions de test de grille et synthétisant 1 sujets théoriques
- ✓ Présentation du mini projet
- ✓ Obtention d'une note minimale 5 pour l'évaluation dans les activités de candidature

Date de remplissage	Responsable des application	Responsable du cours
19.06.2023	Raul Malutan, Maître de conférences	Monica Borda, Professeur des universités

Date d'avis en département 11.07.2023	Directeur du département Virgil Dobrotă, Professeur des universités
Date d'avis par le Conseil de la Faculte d'Electrinique, Telecommunications et Technologie de l'Information 12.07.2023	Doyen Ovidiu Pop, Professeur des universités