Nom de la discipline	Techniques de cryptage et de tatouage
Domaine d'étude	Ingénierie électronique et télécommunications
Master	Traitement du signal et des images - mastère francophone
Code de la discipline	52331411
Titulaire du cours	Prof. dr.ing. Monica Borda – Monica.Borda@com.utcluj.ro
Collaborateurs	Dr.ing. Bogdan Belean – Bogdan.Belean@com.utcluj.ro
Département	Communications
Faculté	Electronique, Télécommunications et Technologie de l'information

Sem.	Type	Cours	Applications			Cours	Applications			Etude individuelle	TOTAL	Credits	Vérification
		[h/semaine.]				[h/semestre.]							
			S	L	P		S	L	P				
3	**Spécialité**	**2**	**-**	**2**	**-**	**28**	**-**	**28**	**-**	**74**	**130**	**5**	**Epreuve écrite**

Compétences acquises

Connaissances théoriques

Protocoles cryptographiques : introduction • protocols pour communications symétriques • protocols pour communications assimetriques et hybrids • protocols pour signatures • protocols pour exchange des clés • protocols pour authentication

Algorithmes cryptographiques : bases mathématiques • algorithmes symétriques - standard DES • autres chiffres (LUCIFER, IDEA, RC2, RC4, AES) • générateurs des séquences aléatoires et pseudo aléatoires • fonctions hache • algorithmes au clés publics • algorithmes pour signatures numériques

Techniques cryptographiques

Applications: techniques de tatouage (watermarking) et steganographie ADN

Aptitudes :

- Connaissance du rôle d'un cryptosystheme
- Connaissance des technologies cryptographiques de base
- Connaissance des attaques et des modèles de sécurité

Connaissances pratiques

- Capacité de comprendre le fonctionnement, le rôle et l'utilisation des algorithmes cryptographiques et les signatures numériques
- Capacité de conception des applications de sécurité

Connaissances nécessaires - mathématiques, théorie de l'information, traitement du signal et des images, circuits analogiques et numériques

A. Cours		
1	Introduction. Objectifs. Historique.	2 heures
2	Cryptographie classique	2 heures
3	Protocoles cryptographiques	2 heures
4	Signatures numériques	2 heures
5	Algorithmes symétriques	2 heures
6	Générateurs des séquences aléatoires et pseudo aléatoires	2 heures
7	Fonctions hache et algorithmes	2 heures
8	Algorithmes au clés publics	2 heures
9	Techniques cryptographiques	2 heures
10	Tatouage: principes.	2 heures
11	Tatouage des images et de la vidéo	2 heures
12	Autres applications du tatouage.	2 heures
13	Steganographie ADN	2 heures
14	Conclusions et préparation de l'examen	2 heures

B1. Applications – **TRAVAUX PRATIQUES** (modules de 4 heures toutes les deux semaines)		
1	TP 1 – Introduction. Description de la plate-forme de laboratoire	4 heures
2	TP 2 – Cryptographie classique	4 heures
3	TP 3 – Algorithmes symétriques	4 heures
4	TP 4 – Cryptographie à clé publique	4 heures
5	TP 5 – Tatouage	4 heures

6	TP 6 – Cryptage des images.	4 heures
7	TP 7 – Cryptographie ADN	4 heures
B2. Salle de TP 210 A Dorobanților 71-73		

C. Etude individuelle						
miniprojet - application en C/C++, article scientifique						
Etude individuelle	Etude cours	Tutoriaux	TPs	Epreuve écrite	Miniprojets	Total
Temps [heures]	14	-	19	3	38	74

Références

1. Titu Băjenescu, Monica Borda- *Securitatea în informatică şi telecomunicații*- Ed. Dacia 2001
2. Bruce Schneier - *Applied Cryptography – Protocols, Algorithms and Source Code in C. Second Edition*- John Willey & Sons, 1996
3. William Stallings – *Cryptography and network security. Principles and practice*- Prentice-Hall, 2nd edition, 1999
4. Alfred J. Menezes, Paul von Oorschot, Scott A. Vanstone- *Handbook of Applied Cryptography* - CRC Press, 1997
5. I. Cox, J. Bloom, M. Miller-*Digital Watermarking: Principles & Practice*- Morgan Kaufmann Publishers, 2001

Examination	
Mode d'examination	Epreuve écrite sans documents(3 heures)
Composantes de la note finale	Mini projet M (M); Examen (E)
Formule de calcul de la note finale	N=0,6E+0,4M si E>4

Titulaire du cours
Prof. dr. ing. Monica Borda

_____