Contenus

Nom du Cours		Semestre du Cours	Cours Théoriques	Travaux Dirigés (TD)	Travaux Pratiques (TP)	Crédit du Cours	ECTS
INF 524		2	3	0	0	3	6

Cours Pré-Requis	
Conditions d'Admission au Cours	

Langue du Cours	Anglais
Type de Cours	Électif
Niveau du Cours	Master
Objectif du Cours	Ce cours présente les techniques modernes de cryptographie (cryptage asymétrique, c'est-à-dire cryptage à clé publique), leur cryptanalyse et leur utilisation. Les programmes informatiques de ces techniques de cryptage sont écrits à la maison dans le cours et les articles importants du cours sont examinés.
Contenus	Semaine 1 : Introduction à la théorie des nombres. Semaine 2 : Propriétés de divisibilité et théorèmes associés. Semaine 3 : Théorèmes de la théorie des nombres. Semaine 4 : Théorèmes de la théorie des nombres. Semaine 5 : Théorèmes de la théorie des nombres. Semaine 6 : Théorèmes de la théorie des nombres. Semaine 7 : Article de Diffie-Helman (1976). Semaine 8 : Article de RSA (1978). Semaine 9 : Théorèmes de l'algorithme RSA. Semaine 10 : Application de l'algorithme RSA. Semaine 11 : Application de l'algorithme RSA. Semaine 12 : Articles sur les algorithmes RSA plus rapides. Semaine 13 : PGP (Pretty Good Privacy). Semaine 14 : Applications sur la cryptographie à clé publique (SSL).
Ressources	1. Ders kapsamındaki orijinal makaleler. 2. Singh, S., “Kod Kitabı”, Klan Yayınları, 2004.

Intitulés des Sujets Théoriques

Semaine	Intitulés des Sujets
1	Introduction à la théorie des nombres
2	Propriétés de divisibilité et théorèmes associés
3	Théorèmes de la théorie des nombres I
4	Théorèmes de la théorie des nombres II
5	Théorèmes de la théorie des nombres III
6	Théorèmes de la théorie des nombres IV
7	Article de Diffie-Helman (1976)
8	Article de RSA (1978)
9	Théorèmes de l'algorithme RSA
10	Application de l'algorithme RSA I

Semaine	Intitulés des Sujets
11	Application de l'algorithme RSA II
12	Articles sur les algorithmes RSA plus rapides
13	PGP (Pretty Good Privacy)
14	Applications sur la cryptographie à clé publique (SSL)