Contenus

Code du Cours	Nom du Cours	Semestre du Cours	Cours Théoriques	Travaux Dirigés (TD)	Travaux Pratiques (TP)	Crédit du Cours	ECTS
INF441	Principes fondamentaux de la Cryptologie	5	3	0	0	3	5

Cours Pré-Requis	
Conditions d'Admission au Cours	

Langue du Cours	Turc
Type de Cours	Électif
Niveau du Cours	Licence
Objectif du Cours	Bien que la cryptographie soit une science très ancienne, elle a récemment connu une véritable révolution. Les techniques de l'arithmétique ont aidé à construire des propriétés dites unidirectionnelles. Par exemple, alors qu'il est très facile à chiffrer pour quiconque connaît la clé publique, il est devenu impossible à déchiffrer pour ceux qui ne connaissent pas la clé privée. Le cryptage moderne est utilisé pour sécuriser l'accès aux ordinateurs, aux systèmes de commerce électronique, aux transactions bancaires, voire pour authentifier un document numérique ou pour le vote électronique. Dans ce contexte, les objectifs de ce cours peuvent être énumérés comme suit : - Enseignement des principaux algorithmes utilisés dans les cryptosystèmes à clé publique: algorithmes "gloutons", algorithme Euclid et algorithmes de calcul rapide en force modulo n - Preuve des principaux théorèmes arithmétiques utilisés dans les systèmes à clé publique - Application des théorèmes aux cryptosystèmes Merkle-Hellman, RSA et El Gamal - Expliquer les fonctionnalités de sécurité des systèmes - Démonstration de la manière dont les systèmes de cryptage sont également utilisés dans les systèmes d'authentification - Présentation des anciens (Ceaser, Vigenère, ...) et des Modernes (mot de passe à usage unique, cryptage Hill) des systèmes de cryptage à clé secrète à l'étudiant - Présentation de différents systèmes de chiffrement par blocs.
Contenus	Semaine 1 Algorithme de Glouton, applications en cryptographie Semaine 2 Algorithme euclidien hebdomadaire et application mod n Semaine 3 Théorèmes de Lagrange et Fermat, applications de calcul rapides et modulaires Semaine 4 Système de cryptage RSA de la semaine Semaine 5 Bloquer le cryptage RSA Semaine 6 Problème de logarithme discret Semaine 7 Méthode d'échange de clés Diffie-Hellman Semaine 8 d'examen à mi-parcours Semaine 9. Système de cryptage de la El Gamal Semaine 10 Fonctions de signature électronique, de signature et de hachage Semaine 11 César, Vigénère, etc. méthodes de cryptage classiques telles que Semaine 12 Cryptage Hill Semaine 13 Principes de la semaine et mécanismes de fonctionnement des chiffrements par blocs Semaine 14 Diagramme de Feistel
Ressources	1.Ders Notları: http://uni.gsu.edu.tr/moodle/course/view.php?id=53 2. Cours de cryptographie, Gilles Zémor, Cassini. ISBN 2-84225-020-6

Intitulés des Sujets Théoriques

Semaine	Intitulés des Sujets
1	Algorithme de Glouton, applications en cryptographie
2	Algorithme euclidien hebdomadaire et application mod n
3	Théorèmes de Lagrange et Fermat, applications de calcul rapides et modulaires
4	Système de cryptage RSA de la semaine

Semaine	Intitulés des Sujets
5	Bloquer le cryptage RSA
6	Problème de logarithme discret
7	Méthode d'échange de clés Diffie-Hellman
8	d'examen à mi-parcours
9	Système de cryptage de la El Gamal
10	Fonctions de signature électronique, de signature et de hachage
11	César, Vigénère, etc. méthodes de cryptage classiques telles que
12	Cryptage Hill
13	Principes de la semaine et mécanismes de fonctionnement des chiffrements par blocs
14	Diagramme de Feistel