UNIVERSITÉ D'EVRY
VAL D'ESSONNE

Unité d'enseignement libre : Histoire de la cryptographie

Règlement du contrôle des connaissances

I. Conditions d'inscription

Article 1 – Préinscription : à partir du 19 septembre auprès du responsable de la formation : Abdelmejid Bayad, au département de mathématiques.
Article 2 – Nombre de places : 30 par semestre.

II. Organisation de la formation

Article 3 - Durée de la formation : 12 semaines. Horaire hebdomadaire : 1h30, le jeudi après-midi.
Article 4 – Cette formation donne droit à deux ECTS.

III. Contrôle des connaissances

Article 5 – L'évaluation s'effectue sous la forme d'un examen en fin de semestre. La présence à toutes les séances est obligatoire.

IV. Organisation des examens

Article 6 - L'absence à l'examen entraîne la note de 0/20. L'examen a lieu à la fin du semestre de la formation. Une session de rattrapage a lieu en septembre.
L'enseignant responsable de la notation se charge de publier les résultats de l'examen.

V. Admission

Article 7 – Responsable de la notation : Abdelmejid Bayad.
Article 8 - Conditions de validation de l'UE : l'UE est validée si la note obtenue à l'examen est supérieure ou égale à 10/20.
Article 9 - Les copies peuvent être consultées sur demande auprès de l'enseignant responsable de la formation, dans un délai maximum d'un mois après la publication des notes.

FICHES DESCRIPTIVES INDIVIDUELLES DES ELEMENTS CONSTITUTIFS

Intitulé de l'EC :		**Histoire de la cryptographie**	**Pré-requis :**	aucun
Semestres :	**123 456**			
Enseignant responsable		Abdelmejid Bayad (département de mathématiques)		

Capacités / compétences générales / compétences spécifiques

La cryptographie etait le domaine réservé des services du chiffre chez les militaires, du code de César à la machine Enigma -.
Elle fait aujourd'hui partie de notre vie quotidienne :
cartes à puce et monétique, Internet et courrier électronique ...
Nous faisons déjà tous de la cryptographie sans le savoir.
La cryptographie est le le moyen d'assurer la confidentialité des communications entre militaires ou entre diplomates ou entre tout simplement deux personnes...etc...
Cette science intéresse donc tout le monde, depuis le lycéen jusqu'au mathématicien le plus chevronné, en passant par le programmeur amateur ou professionnel, sans oublier le responsable de la sécurité d'un réseau informatique
Permettre à chacun de connaître l'histoire de cette science et se familiariser avec, d'en comprendre les mécanismes, tel est l'objectif de ce module.

Contenu de la formation

1) Introduction: Nécessité historique de la cryptographie. 2) Méthodes historiques de cryptographie : - cryptographie par substitution monoalphabétique :principes, code de cesar,Carré de Polybe et histoire des nihilistes russes, Chiffre de Delastelle, ... -cryptographie par substitution polyalphabétique :Carré de vigenère, chiffre de Hill ,....	- Quelques exemples concrets de systèmes cryptographiques et de messages codés : œuvres de Jules Verne, Edgar Alan Poe, Conan Doyle, Cylindre de Jefferson,Cadran d'Alberti.... 3) Méthodes contemporaines DES,AES,RSA :Introduction, notions simples d'arithmétique, puis présentation brève de ces méthodes. 4) Simulations sur ordinateurs.

Modalités pédagogiques :

	heures	**%**
Cours magistraux		
Travaux dirigés	18	50
Travaux pratiques		
TEN		
Projets		
Travail personnel	18	50
		100

	%
Note d'écrit	100
Examens oraux	
Comptes rendus de TP)	
Rapports de projets	
Soutenances orales	
TEN	
	100