TEK-UP
Ecole Supérieure Privée
Technologie & Ingénierie

PLAN D'ETUDES

Deuxième année Ingénieur Informatique

Option : SSIR : Sécurité des Systèmes Informatiques et Réseaux

Semestre 7

Paniers	Modules	ECTS
Cryptologie-1	Initiation à la cryptographie	3
	Sécurité des usages des TIC	3
	Biométrie et tatouage	2
Informatiques-1	Sécurité des systèmes d'exploitation 1	3
	Programmation Python : Développement de logiciels cryptographiques	2
	Sécurité des télécommunications et des Réseaux 1	3
Mathématiques	Arithmétique, Théorie des nombres et courbes elliptiques	2
	Codes Correcteurs	2
	Complexité, Méthodes probabilistes, Structures aléatoires et Optimisation numérique	2
Langues, Communication et Culture d'Entreprise-1	Techniques de communication 1	2
	English Communication 1	2
	Droit d'entreprise	2
Panier transversal-1	Projet Python	2
Total Semestriel		**30**

Panier : Cryptologie-1	Code
	2SSIR-S7-P1

Module : Biométrie et tatouage numérique

Période **Semestre 7** *Charge totale* **21 H**

Responsable	Majdi JRIBI	*email*	Majdi.jribi@ensi.rnu.tn
Équipe pédagogique			

1. Objectifs du module *(Savoirs, aptitudes et compétences)*

Utilisation des modalités biométriques et du tatouage numérique pour assurer la protection et la sécurité des données privées.

2. Prérequis *(autres paniers et compétences indispensables pour suivre le module concerné)*

1. Des notions basiques de l'algorithmiques et des structures de données.
2. Des notions basiques du traitement d'images.

3. Modules du panier

Intitulé du module	*Total*	*Cours*	*TD*	*TP*	*PR*
Biométrie et tatouage numérique	21 h	11h	4 h	6 h	x h

4. Méthodes pédagogiques et moyens spécifiques au panier

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Cours : 11 heures.
- Travaux dirigés : 04 heures.
- Travaux pratiques : 06 heures.

Bibliographie

Titre	Auteur(s)	Editeur/Année	Côte bibliothèque

1- A. Jain, R. M. Bolle, S. Pankanti, Biometrics : Personal Identification in Networked Society, Kluwer Academic Press, 1998.
2- R.M. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha, A.W. Senior, Guide to Biometrics, Springer-Verlag, New York, 2004

3- http ://www.biometricsinfo.org
4- http ://www.europeanbiometrics.info/
5- Patrick Bas. Méthodes de tatouages d'images fondées sur le contenu. Thèse de Doctorat, Institut National Polytechnique de Grenoble, 2000.
6- W. Puech. Safe transfer of image based on color transformation for watermarking. In 4th COST 276 Workshop on Transmitting Processing and Watermarking Multimedia Contents, Bordeaux, France, pages 1–6, march 2003.

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*	Durée allouée	
Introduction à la biométrie	Cours	3H
	TD	0H
	TP	0H
Etude de modalités biométriques	Cours	2H
	TD	1H
	TP	2H
Introduction au tatouage	Cours	3H
	TD	0H
	TP	1H
Étude du tatouage spatial	Cours	1.5H
	TD	1.5H
	TP	1.5H
Étude du tatouage fréquentiel	Cours	1.5H
	TD	1.5H
	TP	1.5H

6. Mode d'évaluation des activités du panier *(nombre, types et pondération des contrôles)*				
Module	*Épreuve écrite*		*Travaux pratiques*	*Projet*
	Devoir	Examen		
			Validation séance par séance	
	Pondération %			
Biométrie et tatouage numérique	25%	60 %	15%	0%

TEK-UP
Ecole Supérieure Privée Technologie & Ingénierie

Fiche Programme Module

Panier : Cryptologie-1	Code
	2SSIR-S7-P1

Module : Initiation à la cryptographie

Période **Semestre 7** *Charge totale* **42 H**

Responsable	Souheib Yousfi	*email*	souheib.youssfi@gmail.com
Equipe pédagogique			

1. Objectifs du module *(Savoirs, aptitudes et compétences)*

La cryptologie : la cryptographie et la cryptanalyse
Les différents types de cryptosystèmes
Les exigences de sécurité à garantir (primitives cryptographiques)

2. Prérequis *(autres paniers et compétences indispensables pour suivre le module concerné)*

Algèbre (des connaissances de base : groupe, corps, division euclidienne, inverse (Théorèmes de Bézout et de Gauss)

3. Modules du panier

Intitulé du module	*Total*	*Cours*	*TD*	*TP*	*PR*
Introduction à la cryptographie	42h	19,5h	7,5h	15h	x h

4. Méthodes pédagogiques et moyens spécifiques au panier

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

Que de la théorie, l'étudiant doit comprendre la cryptographie avant de la pratiquer

Bibliographie

Titre	Auteur(s)	Editeur/Année	Côte bibliothèque

http://www.montefiore.ulg.ac.be/~dumont/pdf/crypto.pdf

https://references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_cryptographiques_v1_20.pdf

https://www.ssi.gouv.fr/uploads/2015/01/FournituresCrypto-v1-2.pdf

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*		Durée allouée
Introduction à la cryptologie	Cours	6H
	TD	0H
	TP	0H
Le chiffrement symétrique: Le chiffrement par bloc et le chiffrement par flux DES,3DES,AES,Dictionnaire de codes (Electronic Code Book, ECB) Enchaînement des blocs (Cipher Block Chaining, CBC) Chiffrement à rétroaction (Cipher Feedback, CFB) Chiffrement à rétroaction de sortie (Output Feedback, OFB) Chiffrement basé sur un compteur (CounTeR, CTR) Chiffrement avec vol de texte (CipherText Stealing, CTS) Compteur avec CBC-MAC	Cours	6H
	TD	3H
	TP	0H
Les chiffrements asymétriques : Elgamal, RSA	Cours	3H
	TD	3H
	TP	0H
Chiffrement à base de courbes elliptiques	Cours	6H
	TD	3H
	TP	0H
Travaux Pratiques sur les algorithmes de chiffrement symétrique, asymétrique et fonction de hachage. Openssl, GPG, OpenVPN	Cours	0H
	TD	0H
	TP	6H
Travaux pratiques sur un protocole d'authentification : Kerberos	TP	3H
	Cours	3H

TEK-UP
Ecole Supérieure Privée
Technologie & Ingénierie

Fiche Programme Module

Panier : Cryptographie-1	Code
	2SSIR-S7-P1

Module : Sécurité des usages des TIC

Période	**Semestre 7**	*Charge totale*	**42 H**

Responsable	Nizar Ben Neji	*email*	nizarbenneji@gmail.com
Equipe pédagogique			

1. Objectifs du module *(Savoirs, aptitudes et compétences)*

Le but de ce cours est d'appréhender l'importance de la sécurité des technologies de l'information et de la communication et de connaître les concepts, les nouveaux paradigmes et les modèles de sécurité les plus utilisés. D'une manière générale, ce cours aide à comprendre l'évolution de l'ingénierie de la sécurité informatique et à dresser un panorama technique des problèmes et des éventuelles solutions pragmatiques et opérationnelles en sécurité.

2. Prérequis *(autres paniers et compétences indispensables pour suivre le module concerné)*

1. Connaissance de base des systèmes d'exploitation et des réseaux

3. Modules du panier

Intitulé du module	*Total*	*Cours*	*TD*	*TP*	*PR*
Sécurité des usages des TIC	42 h	30h	0 h	12 h	x h

4. Méthodes pédagogiques et moyens spécifiques au panier

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Cours
- Travaux pratiques

Bibliographie

Titre	Auteur(s)	Editeur/Année	Côte bibliothèque

http://odile.papini.perso.luminy.univ-amu.fr/sources/SECURITE/cours-SSI-P-II-cours-3S.pdf
http://cosy.univ-reims.fr/~lsteffenel/AdminSGBD/Securite-SGBD.pdf
http://perso.univ-st-etienne.fr/bl16388h/publication2_fichiers/Bossuet_TI2C_2008.pdf

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*	Durée allouée	
I. Introduction à la sécurité a. Objets et objectifs de la sécurité b. Règles de base de la sécurité c. Vulnérabilités et menaces d. Risques d'attaques e. Logiciels malveillants f. Politiques de sécurité g. Référentiels de sécurité dans les TIC	Cours TD TP	4,5H 1,5H 0H
II. Solutions cryptographiques a. Cryptosystèmes cryprographiques b. Hachage cryptographique c. Infrastructure à clés publiques d. Mécanismes de signature électronique e. Monnaie cryptographique et blockchain	Cours TD TP	6H 3H 0H
III. Systèmes de détection et de prévention d'intrusion a. Systèmes de détection d'intrusion machine b. Systèmes de détection d'intrusion réseau c. Solutions SIEM d. Systèmes de prévention d'intrusion IV. Parefeux et Routeurs filtrants a. Déploiement des Parefeux b. Filtrage des paquets IP c. Serveurs mandataires d. Filtrage dynamique et adaptatif e. Translation d'adresses et de ports f. Solutions au contournement du filtrage	Cours TD TP	3H 0H 0H
V. Techniques VPN a. Concept des VPN b. Différents types de VPN c. Protocoles VPN i. PPP ii. PPTP iii. L2TP iv. IPSec v. SSL/TLS VI. Sécurité des systèmes d'exploitation a. Problèmes de sécurité des systèmes d'exploitation	Cours TD TP	3H 0H 3H

b. Points d'entrées des systèmes d'exploitation c. Causes de disfonctionnement d. Menaces des malwares e. Sécurité de la machine i. Sécurité du BIOS ii. Chargeur du système (boot loader) iii. Connexion aux réseaux iv. Verrouillage f. Mécanismes de protection des systèmes d'exploitation i. Contrôle d'accès ii. Gestion des comptes utilisateurs et administrateurs iii. Protection des mots de passe g. Protection des données i. Sécurité par l'obscurité ii. Sécurité par le chiffrement h. Outils de protection i. Antivirus ii. Parefeux iii. Anti-espion iv. Contrôle d'intégrité v. Détecteur d'intrusion		
VII. Sécurité des services Web a. Différents classes d'attaques Web i. Attaques protocolaires ii. Attaques applicatives iii. Attaques sur les postes clients (Navigateurs, Utilisateurs, ...) b. Sécurisation du flux Web: Cas du TLS c. Sécurisation des serveurs Web i. Cas de IIS ii. Cas de Apache d. Sécurisation des applications Web: Cas du PHP e. Scan des applications et identification des vulnérabilités Web f. Sécurité des Webservices i. Niveau XML : XML Encryption et XML Signature. ii. Niveau SOAP : WS-Security, WS-Reliability VIII. Sécurité des réseaux sans fils a. Sécurité en WLAN b. Sécurité en WPAN c. Sécurité en WMAN d. Techniques de protection	Cours TD TP	6H 3H 0H

i. Protection des utilisateurs ii. Protection des terminaux mobiles iii. Protection de l'infrastructure des réseaux sans fil IX. Audit de sécurité a. Démarche d'audit du système d'information i. Interne ii. Externe b. Recueil des informations i. Découverte des réseaux et des équipements actifs ii. Scan des ports et identification des services et des systèmes d'exploitation iii. Collecte des informations à partir des serveurs DNS, SMTP et autres iv. Sniff des paquets v. Accès aux ressources partagées et collecte d'informations utiles vi. Analyse des informations collectées et profiling des systèmes internes vii. Cartographie du réseau interne c. Identification des vulnérabilités i. Scans automatisés des vulnérabilités ii. Identification manuelle des vulnérabilités iii. Tests applicatifs selon les directives OWASP iv. Analyse et classification des vulnérabilités d. Tests de pénétration i. Exploitation des vulnérabilités et acquisition d'accès non autorisés ii. Détournement des mécanismes de restriction iii. Elévation de privilèges et accès aux serveurs critiques iv. Recherche et extraction des informations à partir des bases de données v. Crack de mots de passe online vi. Extraction et crack de mot de passe offline vii. Maintien d'accès et effacement des traces de l'intrusion X. Sécurité du cloud a. Enjeux de la sécurité du cloud computing b. Sécurité des données c. Sécurité de l'infrastructure d. Sécurité des accès réseaux au cloud		
XI. Sécurité dans l'Internet des Objets a. Nouvelles menaces de sécurité	Cours	6H

i. impact sur la vie humaine (voiture connectée, équipement de santé connecté, ...) ii. impact sur la sécurité physique des biens (serrure connectée, caméras, ..) iii. impact sur vie privée (objets perdables, espionnage, ...) iv. dégâts financiers v. attaque destructive à grande échelle (Botnets, SPAM, ...) b. Enjeux techniques de Sécurité dans l'Internet des Objets liés aux i. Changement de contexte (Personnel, Professionnel, Public, ...) ii. Périmètre physique et logique iii. Géo-localisation des objets (Indoor et Outdoor) iv. Limitation des Ressources v. Capacité de traitement vi. Mémoire vii. Bande passante viii. Consommation d'Energie ix. Volume, nature et traitement des données x. Hétérogénéité des architectures et des solutions c. Solutions de Sécurité Adaptées i. Cryptographie Légère ii. Protocoles de Sécurité Adaptés (TLS 1.3, ...) iii. Sécurité logiciel (Validation du code source, Tests intrusifs, ...) iv. Sécurité matériel (Sécurité des systèmes embarqués, Side-channel attacks, ...) v. Sécurité de la transmission des données (Réseaux filaires et sans fil)		

TEK-UP
Ecole Supérieure Privée Technologie & Ingénierie

Fiche Programme Module

Panier : Informatiques-1	Code
	2SSIR-S7-P2

Module : Programmation Python

Période **Semestre 1** *Charge totale* **42 H**

Responsable	Souheib yousfi	*email*	souheib.youssfi@gmail.com
Equipe pédagogique			

1. Objectifs du module *(Savoirs, aptitudes et compétences)*

Concevoir et développer des applications sécurisées en python
Ce module s'articule autour de séances de cours, TP et des mini projets

2. Prérequis *(autres paniers et compétences indispensables pour suivre le module concerné)*

1. Cryptographie1
2. Mathématiques

3. Modules du panier

Intitulé du module	*Total*	*Cours*	*TD*	*TP*	*PR*
Programmation Python : Développement de logiciels cryptographiques	42 h	9h	0h	33 h	x h

4. Méthodes pédagogiques et moyens spécifiques au panier

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

Que de la pratique en utilisant des bibliothèques variées de python, 21h variées et 21h spécifiées

Bibliographie

Titre	Auteur(s)	Editeur/Année	Côte bibliothèque
vermeulen.ca/python-cryptography.html http://www.laurentluce.com/posts/python-and-cryptography-with-pycrypto/ https://launchpad.net/pycrypto			

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*	Durée allouée	
Initiation à la programmation python : les boucles, les listes, les chaines, les tuple,les dictionnaires, les fichiers, les classes et les bases de données.	Cours	9H
	TD	0H
	TP	12H
Utilisation des bibliothèques de cryptographie pour le hachage et le chiffrement. Communication client serveur, The toolkit pycrypto, la bibliothèque Crypto, M2Crypto: A Python crypto and SSL toolkit : RSA, DSA, DH, HMACs, message digests, symmetric ciphers (including AES et DES); SSL afin d'implémenter la communication clients and servers; HTTPS extensions to Python's httplib Mini projet 1 : Utilisation de la bibliothèque random dans le développement d'un jeu de casino. (3h) Mini projet 2 : Chiffrement César et attaque par dictionnaire (6h) Mini projet 3 : Communication client serveur non sécurisée en utilisant les socket, les fonctions de chiffrements de AES, les hachages SHA256 (6h) Mini projet 4 : Le méthodes de chiffrement asymétrique Elgamal et RSA. (6h)	Cours	0H
	TD	0H
	TP	21H

TEK-UP
Ecole Supérieure Privée Technologie & Ingénierie

Fiche Programme Module

Panier : Informatiques-1	Code
	2SSIR-S7-P2

Module : Sécurité des systèmes d'exploitation

Période **Semestre 7** *Charge totale* **42 H**

Responsable	Zied Dridi	*email*	dridi@ati.tn
Equipe pédagogique			

1. Objectifs du module *(Savoirs, aptitudes et compétences)*

Architecture des systèmes d'exploitation (appels système, Kernel, gestion des processus et threads, etc.)

Introduction aux mécanismes de sécurité des OS

Vulnérabilités au niveau OS : buffer overflow, privilege escalation, …

Cas d'étude des systèmes Unix / Linux

2. Prérequis *(autres paniers et compétences indispensables pour suivre le module concerné)*

Architecture des systèmes d'exploitation

Programmation C / C++ / scripting (bash)

Virtualisation

3. Modules du panier

Intitulé du module	*Total*	*Cours*	*TD*	*TP*	*PR*
Sécurité des systems d'exploitation	42 h	6h	0 h	36h	0 h

4. Méthodes pédagogiques et moyens spécifiques au panier

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

Cours : 10 séances

Travaux pratiques

Bibliographie

Titre	Auteur(s)	Editeur/Année	Côte bibliothèque
https://ensiwiki.ensimag.fr/images/b/bc/SecurIMAG-2011-12-07-Mathieu_Blanc-CEA-.pdf			
http://www-lisic.univ-littoral.fr/~poty/Files/Cours_Securite.pdf			

https://shazkhan.files.wordpress.com/2010/10/http__www-trust-rub-de_media_ei_lehrmaterialien_232_main_course20oss.pdf

https://www.ssi.gouv.fr/archive/fr/sciences/fichiers/lti/these-duflot.pdf

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*	Durée allouée	
Module 1 : • Généralités et Rappels système Linux **Filtres** **Personnalisation et utilisation du Shell** **Atelier 1** **Tâches planifiées** **Automatisation de tâches** **Localisation et internalisation** **Atelier 2** **Gestion de l'heure système** **Système de journaux (log)** **Atelier 3** **TCP/IP** **Configuration** **Résolution problème réseaux** **Généralité à propos les noms de domaines** **Atelier 4**	Cours TD TP	6H 0H 3H
Module 2 : PRINCIPES FONDAMENTAUX DE LA SÉCURISATION DU SYSTÈME LINUX **Sécurité au niveau utilisateurs** **Bonnes pratiques d'administration** **Configuration basique de la sécurité système.** **Atelier 5**	Cours TD TP	0H 0H 3H
Module 3 : La sécurité Locale **La sécurité multi-utilisateur** **sudo** **La connexion** **Les mots de passe** **La sécurité pour les utilisateurs** **Les droits**	Cours TP TD	0H 3H 0H

Les ACL **Atelier 6**		
Module 4 : PAM **Approche PAM** **Module PAM** **Atelier 7**	Cours TP	0H 3H
Module5 : SELINUX **Approche** **La sécurité de type TE de SELinux** **Dépannage** **Les politiques de sécurité** **Atelier 8**	Cours TP	0H 3H
Module6 : SSH **Le protocole SSH** **L'authentification à clés publiques** **La configuration de SSH** **Atelier 9**	Cours TP	0H 3H
Module 7 : Audit système **Les attaques** **Logiciels d'audit** **TCPdump, Wireshark** **SNORT** **Atelier 10**	Cours TP	0H 3H
Module 8 : Sécuriser un serveur Linux **Sécuriser un serveur** **Journaux à bord** **Atelier 11**	Cours TP	0H 3H
Module 9 : Paramètres de stratégie de sécurité Windows **Stratégie de compte** **Stratégie locale** **Gestion des paramètres de sécurité basée sur la stratégie** **Stratégie de paramètres de sécurité et stratégie de groupe**	Cours TP	0H 3H

Atelier 12		
Module 10 : BitLocker et Applocker (Windows) **Bitlocker : Approche** **Applocker : Scénarios de sécurité des applications** **Installation Applocker** **Atelier 13**	Cours TP	0h 3H
Module 11 : Sécurité Windows : Quelques Outils **Policy Analyzer** **LGPO** **Atelier 14**	Cours TP	0H 3H
Module 12 : SÉCURITÉ PHYSIQUE **Protèger les accès aux serveurs** **La protection physique des serveurs** **La disquette de secours** **La répartition de charge** **SÉCURITÉ DES DONNÉES** **Les systèmes RAID** **Logical Volume Manager** **Choix du partitionnement** **Les différents filesystem de Linux** **Les sauvegardes et la réplication** **Atelier 15**	Cours TP	0H 3H

TEK-UP
Ecole Supérieure Privée Technologie & Ingénierie

Fiche Programme Module

Panier : Informatiques-1	Code
	2SSIR-S7-P2

Module : Sécurité des télécommunications et des Réseaux 1

Période **Semestre 7** *Charge totale* **42 H**

Responsable	Raki Hammami	*email*	elhammami.raki@gmail.com
Equipe pédagogique			

1. Objectifs du module *(Savoirs, aptitudes et compétences)*

Introduction aux différents types de réseaux
Les mécanismes de sécurité dans la conception au niveau réseau : DMZ, SPOF, équipements de sécurité, architecture n-tiers, etc.
Algorithmes de routage et sécurité : ad-hoc, LAN, Wireless, etc.
Mécanismes de protection périmétrique : filtrage par firewall

2. Prérequis *(autres paniers et compétences indispensables pour suivre le module concerné)*

1. Notions de réseau
2. Connaissance des algorithmes de routage
3. Connaissances des couches OSI et plus particulièrement les couches liaison, réseau et transport
4. ARP et TCP/IP

3. Modules du panier

Intitulé du module	*Total*	*Cours*	*TD*	*TP*	*PR*
Sécurité des télécommunications et des Réseaux 1	42 h	30 h	3 h	9 h	0 h

4. Méthodes pédagogiques et moyens spécifiques au panier

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Cours : 10 séances de cours théorique
- Travaux dirigés :
- Travaux pratiques en laboratoire : Réalisation de filtrages réseaux et test d'ACL / attaque sur les algorithmes de routage / détournement de trafic / VLAN hopping

Bibliographie

Titre	Auteur(s)	Editeur/Année	Côte bibliothèque

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*	Durée allouée	
Rappel TCP/IP et notions de bases	Cours	
	TD	
	TP	
Introduction à la sécurité Etat des lieux de la cybercriminalité Objectifs de la sécurité Vocabulaire et définitions Menaces et motivations	Cours	
	TD	
	TP	
Les attaques connus : catégories et mode opératoire TP1 : Mettre en évidence quelques techniques d'attaques classiques • LAB1 : Cracking et test de robustesse de mot de passe • LAB2 : Sniffing et vol d'informations d'authentification • LAB3 : ARP Spoofing et mise en œuvre de l'attaque Man in the Middle • LAB4 : Attaque DoS via SynFlooding	Cours	
	TP	
	TD	
NAT, Contrôle d'accès et filtrage	Cours	
1. Les différents mécanismes de la translation d'adresses (NAT&PAT) TP2 : Configuring Dynamic and Static NAT 2. Le contrôle d'accès via les listes d'accès ACL TP3: Configuring IP ACLs to mitigate Attacks 3. Les pare-feu :	TP	

a. Rôle, types et les différents types de filtrage b. Règles de sécurité et principe de fonctionnement 4. Les pare-feu applicatifs : Proxy et Reverse Proxy 5. Architecture de sécurité et scénarios de déploiement TP4 : Mettre en place d'une architecture sécurisée ·LAB1 : Installation IPCOP et mettre en place la politique de sécurité ·LAB2 : Installation d'un Proxy Squid sous IPCOP et configuration des restrictions ·LAB3 : Administration d'un FW Cisco ASA via CLI et GUI		
Cloisonnement et segmentation logique TP5 : Configuration entre des réseaux virtuels (VLANs)		
Hardening des équipements réseaux et bonnes pratiques : illustration des risques et les solutions envisageables 1. Hardening de la couche de management TP6 : Security Hardening Checklist for Cisco Devices in 10 Steps 2. Hardening de la couche de données TP7 : Configuring Port Security 3. Hardening de la couche de contrôle TP8 : Basic Security Configuration		
Haute disponibilité et répartition de charge TP9 : Mise en place du protocole HSRP		

TEK-UP
Ecole Supérieure Privée Technologie & Ingénierie

Fiche Programme Module

Panier : Mathématiques	Code
	2SSIR-S7-P3

Module : Arithmétique, Théorie des nombres et courbes elliptiques

Période	**Semestre 7**	*Charge totale*	**21 H**

Responsable	Habib Bouhaffa	*email*	habibbouhafa@yahoo.fr
Equipe pédagogique			

1. Objectifs du module *(Savoirs, aptitudes et compétences)*

Structures algébriques : groupes, anneaux et corps
Problème du logarithme discret
Problème de la factorisation des nombres

2. Prérequis *(autres paniers et compétences indispensables pour suivre le module concerné)*

1.

3. Modules du panier

Intitulé du module	*Total*	*Cours*	*TD*	*TP*	*PR*
Arithmétique, Théorie des nombres et courbes elliptiques	21 h	9h	6h	6h	0 h

4. Méthodes pédagogiques et moyens spécifiques au panier

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Logiciel Sage : https://sagecell.sagemath.org/ (version en ligne) outil open source

Bibliographie

Titre	Auteur(s)	Editeur/Année	Côte bibliothèque

http://stephane.gonnord.org/PCSI/Algebre/STRUCTURES.PDF
http://licence-math.univ-lyon1.fr/lib/exe/fetch.php?media=exomaths:exercices_corriges_groupe.pdf (exercices corrigés)
http://ljk.imag.fr/membres/Bernard.Ycart/mel/sa/sa.pdf
https://www.math.univ-paris13.fr/~boyer/enseignement/arith-p13/cours.pdf (théorie des nbres)
http://documents.epfl.ch/users/l/la/lassueur/www/numbertheory/Nbr.pdf
http://math.univ-lyon1.fr/~wagner/coursDelaunay.pdf
http://www.lix.polytechnique.fr/~smimram/docs/prepa/tipe-ecc.pdf (courbe elliptique)

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*	Durée allouée	
Rappels d'arithmétique : Nombres premiers et factorisation, Congruences Théorème d'Euleur et petit théorème de Fermat	Cours	3H
	TD	1,5H
	TP	0H

Algèbre : Groupe et sous groupe, Corps de nombres et anneaux d'entiers	Cours	3H
	TD	3H
	TP	3H
Courbe elliptique : Loi de groupe, problème du logarithme discret, choix de la courbe, les points de la courbe. La pratique avec l'outil sage	Cours	3H
	TP	1,5H
	TD	3H

TEK-UP
Ecole Supérieure Privée
Technologie & Ingénierie

Fiche Programme Module

Panier : Mathématiques	Code
	2SSIR-S7-P3

Module : Codes correcteurs

Période	**Semestre 7**		*Charge totale*	**21 H**			

Responsable	Yousfi Souheib	*email*	souheib.youssfi@gmail.com
Equipe pédagogique			

1. Objectifs du module *(Savoirs, aptitudes et compétences)*

L'objectif du cours est de former aux fondements informatiques et mathématiques pour fournir des garanties sur la confidentialité, l'intégrité et l'authentification des communications numériques. Ce cours présente la théorie des codes, ses fondements mathématiques et ses applications en protection de l'information, en compression et en codage canal. Il permet d'acquérir les fondements nécessaires pour la mise en œuvre et l'exploitation des protocoles de codage.

2. Prérequis *(autres paniers et compétences indispensables pour suivre le module concerné)*

1- Connaissances de base en : probabilités.

2- Algorithmique et analyse de coût

3- Bases en algèbre linéaire (résolution de systèmes par élimination de Gauss), arithmétique entière et polynomiale (primalité, pgcd).

3. Modules du panier

Intitulé du module	*Total*	*Cours*	*TD*	*TP*	*PR*
Codes correcteurs	21 h	9 h	12h	0h	0h

4. Méthodes pédagogiques et moyens spécifiques au panier

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Cours
- Travaux dirigés

Bibliographie

Titre	Auteur(s)	Editeur/Année	Côte bibliothèque

http://deptinfo.unice.fr/twiki/pub/Linfo/Organisation%20Rapports/Knoff-Gargne-Lecourtois.pdf

http://197.14.51.10:81/pmb/TELECOMMUNICATION/Theories%20des%20codes.pdf

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*	Durée allouée	
Généralités et Définitions :	Cours	3H

- Quantité d'information - Entropie - Exemple d'application	TD TP	1.5H 1.5H
Codage Source : Compression de l'information - Codage régulier, déchiffrable, irréductible - Construction des codes binaires irréductibles - Paramètres caractéristiques d'un code : Longueur, Capacité, Efficacité - Code de Shannon - Code de Huffmann - Comparaison des codes	Cours TD TP	3H 1.5H 1.5H
Codage Canal : Redondance de l'information - Principe des codes en blocs : codage et décodage - Paramètres des codes en blocs - Codes linéaires : distance de Hamming, détection et correction des erreurs, contrôle de parité - Codes cycliques	Cours TD TP	3H 3H 3H

6. Mode d'évaluation des activités du panier *(nombre, types et pondération des contrôles)*

Module	*Epreuve écrite*		*Travaux pratiques*	*Projet*
	Devoir	Examen		
	Pondération %			
	40 %	60 %	x %	x %

TEK-UP
Ecole Supérieure Privée Technologie & Ingénierie

Fiche Programme Module

Panier : Mathématiques	Code
	2SSIR-S7-P3

Module : Complexité d'Algorithmes

Période **Semestre 7** *Charge totale* **21 H**

Responsable	Yosr Bali	*email*	yosr.slama@gmail.com
Equipe pédagogique			

1. Objectifs du module *(Savoirs, aptitudes et compétences)*

La résolution efficace des problèmes de grande taille, se posant dans les sciences appliquées, exige la conception d'algorithmes adéquats dont l'évaluation des performances, à travers l'analyse de leur complexité, est primordiale. L'objectif de ce cours est la présentation d'une approche générale d'analyse de complexité (temporelle) d'algorithmes, exacts ou d'approximation, de structure itérative (nids de boucles DO) ou récursive. La méthodologie adoptée est illustrés à travers l'étude d'algorithmes appropriés pour la résolution de problèmes types.

2. Prérequis *(autres paniers et compétences indispensables pour suivre le module concerné)*

1. Algorithme

3. Modules du panier

Intitulé du module	*Total*	*Cours*	*TD*	*TP*	*PR*
c	21 h	12h	9h	0h	x h

4. Méthodes pédagogiques et moyens spécifiques au panier

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Cours
- Travaux dirigés

Bibliographie

Titre	Auteur(s)	Editeur/Année	Côte bibliothèque

https://www.labri.fr/perso/duchon/Teaching/ENSEIRB/AlgoProba/Poly.pdf

https://perso.esiee.fr/~buzerl/ENSEIGNEMENT/IN311/poly_in311.pdf

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*	Durée allouée	
1. Introduction générale et concepts de base	Cours	3H
	TD	0H
	TP	0H
2. Evaluation de complexité d'algorithmes itératifs	Cours	3H
	TD	3H
	TP	0H
3. Evaluation de complexité d'algorithmes récursifs	Cours	3H
	TD	3H
	TP	0H
4. Complexité des problèmes-Algorithmes exacts et d'approximation	Cours	3H
	TP	0H
	TD	3H