

CRYPTIS

FORMATIONS EN CRYPTOLOGIE
ET SÉCURITÉ DE L'INFORMATION

Entrez au cœur de la sécurité de l'information

Master Sécurité de l'Information et Cryptologie Pré rentrée 2014-2015

CRYPTIS



Université
de Limoges

FACULTÉ
DES SCIENCES
ET TECHNIQUES

Promotion 2014-2015

- 45 élèves: 27 SI et 18 MCCA
- Taux de sélection
 - 35% MCCA (62 demandes)
 - 19% SI (163 demandes)
 - M1 50%, 3IL 50%, CEF 13%, CVTIC 2%
- Salle de TP spécialisée réservée master Cryptis (bâtiment physique)
- Un panneau d'affichage (liste des soutenances)
- Une salle de travail de groupe à l'étage
- www.unilim.fr/pages_perso/francois.arnault/cryptis.php

Les métiers

- Administration / sécurité des systèmes et réseaux
- Ingénieur en cryptographie
- Auditeur ou consultant en sécurité informatique
- Étude et développement d'applications sécurisées
- Architecte en sécurité
- Ingénieur de certification / évaluateur
- ...

Après un doctorat:

- Enseignant chercheur en informatique
- Enseignant chercheur en mathématiques

Spécificités (I)

- Un diplôme, deux parcours :
 - Sécurité informatique (SI)
Responsable: Philippe Gaborit
 - Mathématiques, cryptographie, codage, et applications (MCCA)
Responsable: François Arnault
- Synergie maths-info
 - Un tronc commun
 - Des options communes
 - Projets en groupes « mixtes », stages, débouchés
- Un large choix de cours
 - Vous précisez votre orientation à travers le choix de vos options
 - Nécessité d'une cohérence dans vos choix

Spécificités (II)

- Master indifférencié
 - Insertion professionnelle immédiate
 - Possibilité de poursuite en thèse
- Une équipe pédagogique formée d'enseignants chercheurs
- Implication de professionnels reconnus
 - 22 intervenants en 2012-13
- Une pédagogie basée sur la pratique
 - Projets en petits groupes, TP.
- Un réseau de diplômés
 - DEA ouvert en 86, DESS en 2000.
 - Associations de diplômés: ADDMUL & ADELCOM



Stages

- De 4 à 6 mois, entre début mars et fin septembre
 - 30 ECTS (tous les crédits du semestre 2)
 - En entreprise, laboratoire de recherche ou organisme public
 - Pas de compensation entre semestres
- Soutenances de la promotion précédente en cours,
 - Regardez le panneau d'affichage,
 - Très fortement recommandé d'assister aux soutenances, (indication du contenu des rapport, d'une présentation, contact avec les encadrants...)
- Offre de stages très large : 200 à 300 offres (mi-novembre 159 offres)
- Responsable : Philippe Gaborit

Calendrier

Jusqu'au 12 septembre : soutenances de stages de la promotion précédente.

- Semestre 1: 15 septembre - mi février (google calendar) ;
- Fin des cours: mi janvier.
 - Révisions, examens et projets.
- Stage: début mars – fin septembre.
 - Au moins 4 mois ; au plus 6 mois. Doit être achevé avant fin septembre.
 - Il est de votre responsabilité de trouver un stage.
 - Mindef, Anssi, se déplacent à Limoges

Équipes de recherche locale

- *Smart Secure Devices (SSD) secinfo.msi.unilim.fr*
 - Recherche sur le thème des objets mobiles de sécurité: carte à puce, TPM, PDA, téléphone portable
 - Sécurité des systèmes, attaques logiques et physiques

- *Protection de l'Information, Codage et Cryptographie*
 - Cryptographie, codes correcteurs d'erreurs, génération d'aléa.
 - Cryptographie basée sur les réseaux.
 - Protection de la vie privée, anonymat.
 - Cryptographie/Information quantique.



Et aussi: *TAN, CF, MOD, SIR.*

Votre futur métier ?

- Soutenances de stage de la promotion sortante :
- Certains rapports de stages sont disponibles à la consultation.
- Discuter avec les enseignants professionnels.
- Séminaire Cryptis le mardi après midi (ce n'est pas une option) salle XLIM 203.
- Suivre les annonces sur www.cryptis.fr mais aussi via la mailing list

Partenariats académiques

- Université de Sherbrooke (Canada) et Chicoutimi (Canada)
 - Cursus intégré (parcours SI)
- Université Mohammed V (Rabat)
 - Cursus intégré (parcours MCCA)
- Convention 3IL
 - Certains élèves de 3ième année intègrent le parcours SI.

Les UE obligatoires

Tronc commun:

30 h – 3 crédits: Organisation de l'entreprise.

30 h – 3 crédits: Anglais.

45 h – 3 crédits: Mécanismes cryptographiques et applications.

30 h – 3 crédits: Développement logiciels cryptographiques.

SI seulement:

105 h – 9 crédits: Administration et Sécurité des Systèmes et Réseaux.

MCCA seulement:

45h – 4,5 crédits: Cryptographie à clés secrètes.

45h – 4,5 crédits: Cryptographie à clés publiques.

Un semestre = 30 ect

OB = 21 ect



SI
9 ect

Tronc commun
12 ect

MCCA
9 ect



SI
{3,3,3,3,6} ect

Tronc commun
{6 (3+3), 3} ect

MCCA
{3,3,3} ect

OPT = 9 ect

Les UE optionnelles (I)

Tronc commun

30 h – 3 crédits: Cartes à puces et Java Card, développement

30 h – 3 crédits: Cartes à puce, attaques physiques

30 h – 3 crédits: Certification et développement sécurisé.

Les UE optionnelles (II)

SI seulement:

30 h – 3 crédits: Sécurité applicative.

30 h – 3 crédits: Méthodologie pour la sécurité.

30 h – 3 crédits: Terminaux mobiles communicants.

xx h – 6 crédits: 3IL

MCCA seulement:

30 h – 3 crédits: Codes correcteurs et cryptographie.

30 h – 3 crédits: Théorie des nombres.

30 h – 3 crédits: Outils mathématiques émergents pour la cryptographie.

UE optionnelles communes

Carte à puces et Java Card

- *Responsable: Damien SAUVERON & Christophe CLAVIER*
- 30 h – 3 crédits et 30h – 3 crédits
- Norme ISO 7816 régissant l'interopérabilité des cartes à puce.
- Applications industrielles, architecture, spécifications. Carte bancaire, téléphonie, télévision à péage,...
- Attaques spécifiques sur carte : analyse de la consommation de courant, du temps de calcul. Contre-mesures.
- Java Card 3.0.
 - TP sur cartes / Un projet par équipe.
- Intervenants externes : gemalto, Inside
- MCC : TP – Rapport – Ecrit

Certification et développement sécurisé

- *Responsable: Damien SAUVERON*
- 30 h – 3 crédits – (21/9/0)

L'objectif de cette UE est d'apprendre aux étudiants à identifier les points essentiels à sécuriser lors du développement d'un logiciel ou matériel informatique. Pour cela ils seront sensibilisés aux différentes propriétés de sécurité pouvant être mises en œuvre sur un produit et aux méthodes permettant de s'assurer de leur efficacité. En particulier, on abordera :

- la définition d'une analyse de risque (identification des menaces, des hypothèses d'utilisation du produit, etc.) ;
- les méthodes de mise en place de contre-mesures efficaces et exhaustives;
- les méthodologies de développement permettant d'augmenter et d'évaluer la confiance (les Critères Communs par exemple) ;

A la fin de l'UE l'étudiant devrait être à même de pouvoir concevoir un produit grâce à une démarche méthodique qui permettra à un éventuel tiers d'avoir confiance dans le produit en question.

- Intervenants:
- MCC : projet, écrit

UE optionnelles – Parcours SI

Sécurité applicative

- *Responsable: Olivier Blazy*
- 30 h – 3 crédits – (15/15/0)

Cette UE traite de la sécurisation globale d'une application, que ce soit dans ces aspects système ou réseau. Les cas considérés pourront être choisis parmi :

- Sécurité des messageries électroniques,
- Sécurité des sites Internet: menaces, architecture, sécurisation. Exemple des plateformes de commerce électronique.
- Sécurité de la téléphonie sur IP, mobilité et utilisateurs nomades.
- Sécurité des services web, gestion des identités.
- Gestion des droits numériques (DRM): architecture, principe de fonctionnement, limitations

- Intervenant:
- MCC: un partiel, un écrit final.

Méthodologie pour la sécurité

- *Coordonnateur: Marc RYBOWICZ*
- 30 h – 3 crédits – (30/0/0)

Sensibilisation aux aspects organisationnels de la sécurité de l'information d'un organisme:

- Politique de sécurité
- Analyse de risques
- Système de management de la sécurité de l'information

Panorama des méthodes et approches possibles : ISO 7498-2, ISO 27000, EBIOS, MEHARI,....

- Intervenants : professionnels (Orange, Byward, etc).
- MCC: Ecrit.

Terminaux mobiles communicants

- *Responsable: Pierre François BONNEFOI*
- 30 h – 3 crédits - (15/0/15)
 - étude des plateformes d'exécution : carte à puce, assistant personnel, téléphone mobile ;
 - les techniques de communication sans fil : Bluetooth et WiFi ;
 - la mobilité dans les réseaux avec infrastructure (GSM et IPv6) et le routage dans les réseaux ad hoc ;
 - mobilité de code : serveur d'application, systèmes multi-agents ;
 - programmation; sécurisation du code et des accès ;
- Intervenants :
- MCC: projet, écrit

Choix d'options SI

- **Audit ou consultant sécurité :**

3 crédits: Organisation et méthodes de la sécurité.

3 crédits: Certification.

3 crédits: Sécurité applicative

- **Etude et développement d'applications sécurisées:**

6 crédits: Cartes à puces et Java Card.

3 crédits: Sécurité applicative

3 crédits: Certification

- **Ingénieur systèmes et réseaux**

3 crédits: Certification.

3 crédits: Organisation et méthodes de la sécurité.

3 crédits: Terminaux mobiles communicants.

- **Panachage possible**

3 x 3 crédits à choisir dans les UE pré citées
Attention à l'EDT il peut il y avoir des incompatibilités

UE obligatoires – Parcours MCCA

Cryptographie à clé secrète

- *Responsable: Thierry BERGER*
- 45 h – 4,5 crédits – (21/17,5/7,5)
- Fonctions Booléennes, critères cryptographiques (degré algébrique, résilience...)
- Chiffrement par bloc: conception, cryptanalyse
- Chiffrement à flot et générateurs pseudo-aléatoires: conception et cryptanalyse.
- Fonctions de hachage, chaînage
- Cryptanalyse linéaire, différentielle, distingueurs.
- Intervenants: P. Gaborit, T. Berger
- MCC: écrit + TP

Cryptographie à clé publique

- *Responsable: François ARNAULT*
- 45h – 4.5 crédits – (21/17,5/7,5)
- Analyse et conception des systèmes à clé publique (RSA, Diffie-Hellman, El Gamal, courbes elliptiques). Sécurité.
- Algorithmes en Théorie des Nombres (Factorisation et logarithme discret)
- Preuves de sécurité. Modèle des oracles aléatoires. Sécurité sémantique.
- Zero-Knowledge (Fiat-Shamir, Schnorr, GQ). preuves interactives.
- Sécurité des générateurs aléatoires. Générateurs prouvés sûr.
- Intervenants:
- MCC: Partiel + Ecrit final

UE optionnelles – parcours MCCA

Théorie des nombres

- *Responsable: Chazad MOVAHHEDI*
- 30 h – 3 crédits – (15/15/0)

- Introduction à la théorie algébrique des nombres: anneaux des entiers des corps de nombres, discriminant et ramification, unités et groupes des classes d'idéaux, exemples des corps quadratiques et cyclotomiques

- MCC: partiel + écrit

Codes correcteurs et cryptographie

- *Responsable: Thierry BERGER*
- 30 h – 3 crédits – (15/15/0)
- Codes MDS, codes de Reed-Solomon, codes RS généralisés.
- Sous-codes sur un sous corps, codes BCH, codes de Goppa
- Décodage des codes de la famille Reed-Solomon, list decoding.
- Codes LDPC, codes convolutifs, décodage souple, décodage itératif.
- Schéma cryptographique de McEliece, signature, schéma de Stern.
- Intervenants: P. Gaborit, T. Berger
- MCC: écrit + mémoire

Outils mathématiques émergents pour la cryptographie

- *Responsable: François Arnault*
- 30 h – 3 crédits – (15/15/0)

L'objectif de cette UE est de présenter les outils mathématiques émergents en cryptographie. Le contenu de cette UE est amené à changer d'une année sur l'autre. Thèmes cette année :

- Cryptographie basée sur les réseaux euclidiens (Vinatier, Gaborit)
- Bases de Gröbner et cryptographie (Olivier Ruatta).
- Théorie de l'Information et Cryptographie Quantiques

- Intervenants: O. Ruatta, P. Gaborit, S. Vinatier, F. Arnault
- MCC: projet sur le thème de votre choix.

Choix d'options MCCA

- **Crypto mathématique renforcée :**

3 crédits: Codes correcteurs et cryptographie

3 crédits: Outils mathématiques émergeants pour la cryptographie.

3 crédits: Théorie des nombres.

- **Carte à Puces :**

6 crédits: Cartes à puces et Java Card.

3 crédits: Certification et développement sécurisé ou Méthodologie pour la sécurité.

- **Panachage possible:**

3 crédits: Cartes à puces et Java Card.

3 crédits: Codes correcteurs et Crypto ou Outils mathématiques ou

3 x 3 crédits à choisir dans

- Codes correcteurs et cryptographie
- Outils mathématiques émergeants
- Théorie des nombres
- Certification et développement sécurisé
-

etc...

Pédagogie

- Travaux en groupes (projets)
 - Certains en équipe mixte (étudiants des deux parcours)
- Intervention de professionnels extérieurs à l'université
- Exemples de sujets:
 - Attaques physique et logiques sur une carte à puce, [3 publications scientifiques par des étudiants],
 - Reverse complet d'un OS de carte,
 - Déploiement de réseaux sécurisés,
 - Écriture d'exploits,...

Bourses au mérite

- Une bourse par parcours (SI et MCCA) 3k€
 - Pour tout type d'étudiants (boursiers sur critère social ou non) mais s'engageant à poursuivre en doctorat (engagement écrit) et choisis par concours sur leurs résultats universitaires précédents.
 - En cas d'égalité sur les critères d'excellence, les critères sociaux seront pris en compte.
 - Dossier à envoyer à François Arnault (MCCA) et Philippe Gaborit (SI).
 - Echéance 15/09

- **Stages** : Gemalto, Trusted Logic, Thales Security Group, Ministère de la Défense, Ministère de l'Intérieur, Crédit Lyonnais, INRIA (LORIA, IRISA), Ace Europe, Cap Gemini Ernst & Young, Dictao, Orange, Sogeti, IdealX, LASER Cofinoga, Bertin Technologies, Atos Worldline...
- **Embauches** : Ministère de la Défense, Ministère de l'Intérieur, ACE Europe, Amesys, Bertin Technologies, Bull SA, Orange Business (CVF), Cap Gemini Ernst & Young, Dictao, Orange, Ilex, Trusted Labs, Unilog, Byward, Sogeti...

Questions ?

,