# Welcome to M2 SCCI 2014-2015

## Promotion David Albert Huffman

David A. Huffman(1925-1999) [Photo: Don Harris]

Grenoble INP

UNIVERSITE JOSEPH FOURIER

Grenoble University

# SCCI - M2P / M2R *Security, Cryptology and Coding of Information Systems*

## - Sécurité, Cryptologie et Codage des Systèmes d'Information

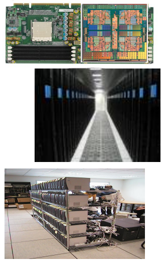
- Context
- General presentation
  - 1. Academic program, calendar
  - 2. Lectures/Tutoring organization
- Administration, registration: *who's who*

# Context - Objective

- **Context** : expansion of networks and distributed applications

  - *Confidentiality, Authentication, Integrity, Non-repudiation*

- Various applications and professional skills:



  - **Enterprise specialised in security:** solutions providers (hardware, software, smartcard, …); security audit, …
  - **Specialized department of a company :** bank, e-business, telecom,tv, …
  - **Information system within a company:** network/system administration

**1 year dedicated program at Grenoble University** (UJF+INP)
*Ensimag, Institut Fourier, UFR IMAG*

- **Objective** : formation of experts in security and coding technologies
  - **Cryptology** : mathematical protocols (RSA, AES, ECC…)
  - **Security**: software/hardware (network, system, integraton)
  - **Applications** : watermarking, multimedia, smartcard, …
- **M2P** : Directed to profession: sept-march=lectures+training / apr-sept project
- **M2R** : Directed to research: sept-jan=lectures+training / feb-june project

# Brief history & organization

- Master UJF-INPG  Cryptologie, Sécurité, Codage de l'Information (2001…)
  - Sept 2003: first promotion: 17 graduate students
  - **275** graduate students up to sept 2014,
  - From Sept 2007: international M2P – program taught in English
  - From sept 2008: part of MOSIG International Master;
  - Sept 2011: 10 years birthday :  **http://10ans-scci.imag.fr/**
  - From sept 2011: "M2P, M2R, ( SAFE )

- **M2P+R Security, Cryptology and Coding of Information Systems**

  - Gathers French and English speaking students (2 groups of students)
  - **Director  UJF/IF :** Philippe.Elbaz-Vincent, , Vanessa Vitse at ujf-grenoble.fr,
  - **Director INP/ENSIMAG:** Jean-Louis.Roch at imag.fr
  - Web:
    - http://www-ufrima.imag.fr/spip.php?article49
    - http://www-ufrima.imag.fr/spip.php?article49
    - http://www-fourier.ujf-grenoble.fr/enseignement/spip.php?rubrique19

# Calendar 2014-2015

## M2P

- mid-Sept->March: courses (level 3) [2 weeks optional pretraining early sept]
- April -> September : (level 4) full-time internship (Master thesis)
  - mid-june: mid-term presentation
    - In English !
  - mid-september: defense

## M2R

- mid-Sept->January: courses (level 3)
- February-> June: (level 4) full-time internship (Master thesis)
  - mid-june: defense

- **Validation: by “level”** (~semester)
  - Mark ≥ 10/20=50% to level 3 (courses)
    - No mark < 7 in global units
  - Mark ≥ 10/20=50% to level 4 (thesis/project)

- **Warning ! Internships must be validated** by Ph. E-V / V. V (for UJF) or J.-L. R (for INP).

**Furthermore, academic supervisor for the internships are also chosen by the directors.**

# M2P and M2R courses

- Common core: cryptology and security [15 ECTS]
    - Models for security
    - Symmetric and asymmetric cryptology - PKI infrastructures
    - System administration and network security
- Elective specialization [12 ECTS] : choose one between
    - Security of Information Systems [12 ECTS]
        - Advanced system and network security
        - Secure hardware architecture
        - Distributed algorithms and fault-tolerance
        - Secure infrastructure deployment project
    - Cryptology, coding and multimedia applications [12 ECTS]
        - Advanced cryptology: elliptic curves, cryptanalysis
        - Multimedia applications, watermarking
        - Coding and fault-tolerance
- Elective course unit [3 ECTS] : choose one between
    - Smart card security; audit and normalization [3 ECTS]
    - New trends in cryptology: quantum, biometrics, pairings [3 ECTS]
- Master thesis [27 ECTS]

- Note: early september: Specific optional introduction courses
    - Math [group theory,arithmetics]; linux & programming ; information systems [UML]

# Academic Program
# M2P SCCI (M2-P)

- **27 ECTS Master thesis**
- **3 ECTS UE Transversal (English / French / … )**
- **30 ECTS “scientific/technology”**
  - 15 ECTS Common Core
  - 12 ECTS Elective Specialization in Security (“math” or “info”)
  - 3 ECTS = elective unit (2 proposed, but yet open to all units proposed in Grenoble M2 Math-Info)

Grenoble INP

UNIVERSITE JOSEPH FOURIER

# Security, Cryptology and Coding of Information Systems

## M2P SCCI – 2014/2015 Academic Program

| *Non-elective Core Courses  18 ECTS* | ECTS | Teaching teams |
|---|---|---|
| - **Security models: proofs, protocols and politics** | 6 | Autreau, Kumar, Lakhnesh,  Roch |
| - **Symmetric and asymmetric cryptology – PKI** | 6 | Dumas, Duval, Elbaz-Vincent and guests |
| - ***System administration and network security*** | 3 | Mounié, |
| - **English or French** | 3 | Pool Langues |
| ***Choose one of the two  following elective 12 ECTS*** | | |
| **Elective A. Security of systems and infrastructures**<br>- ***Advanced security of system and networks***<br>- **Hardware and embedded secure architectectures**<br>- **Distributed algorithms and fault-tolerance**<br>- **Deployment of a secure grid infrastructure** | <br>3<br>3<br>3<br>3 | <br>Wagner, Castellucia<br>Maisri<br>Lachaize,<br>Wagner |
| **Elective B. Cryptology, coding and multimedia**<br>- **Advanced cryptology:elliptic curves, cryptanalysis**<br>- **Multimedia applications and watermarking**<br>- **Error correcting codes and fault-tolerance** | <br>6<br>3<br>3 | <br>Vitse<br>Cayre, Ebrahimi<br>Pernet; Roch; Patchichkine, Brossier |
| ***Choose one of the two  following elective 3 ECTS*** | | |
| - **Elective 1. Smart card security, certif. and norms** | 3 | Autreau, Clediere, Rhué |
| - **Elective 2. New trends in cryptography** | 3 | Malha, Mainguet, Vitse |

# Academic Program

## M2R SCCI

- **27 ECTS Master  thesis**
- **3 ECTS UE Transversal (English / French / … )**
- **30 ECTS “scientific/technology”**
  - 24 ECTS Common Core
  - 6 ECTS elective unit (2 units of 3 ETCS proposed, but yet open to all units proposed in Grenoble M2 Math-Info)

# Security, Cryptology and Coding of Information Systems

## M2R SCCI – 2014/2015
## Academic program

| *Non-elective Core Courses 18 ECTS* | ECTS | Teaching teams |
|---|---|---|
| - **Security models: proofs, protocols** | **6** | Lakhnech, Roch |
| - **Symmetric and asymmetric cryptology – PKI** | **6** | Dumas, Duval, Elbaz-Vincent and guests |
| - **Security of computer systems and networks**<br>* *System administration and network security (3)*<br>* *Advanced security of system and networks (3)* | **6** | Castellucia,, Wagner |
| - **Advanced cryptology:elliptic curves, cryptanalysis** | **6** | Vitse |
| - **English or French (FLE)** | **3** | Pool Langues |
| ***Elective scientific module/units : 6 ECTS***<br>- Requires validation from M2R SCCI academic supervisors. Timetable compatibility is guaranteed for both following units (3 ECTS each) :<br>* Smart card security, certif. and norms (3 ECTS)<br>* New trends in cryptography (3 ECTS) | **6** | Autreau, Clediere, Rhué<br>Malha, Mainguet, Vitse |
| - **M2R Thesis** | **27** | |

# Courses and M2P trainings

- **1 ECTS Scientific Unit = 10h attendency M2**
- Courses slots of 1.5 hours per week per student:
  - 8h-9h30 / 9h45- 11h15 / 11h30-13h
  - 13h45-15h15/15h30-17h

- M2P 3 ECTS = 30H classes / 45H practical work + Homework
  - **18h lectures in English** (~ 2 slots of 1h30 / week)
  - + ***12h "training"*** : TP/ Exercises/complts
    - If enough students, may be given twice:
      1 group in English + 1 group in French
    - => for each unit, choose either French or English, once!
- M2R: courses, homework, no training / TP
- Additional tutoring (office hours)
  - on request: see your professors

# Elèves-ingénieur (inscription en 3A -pas Master-)

- Programme = M2 (P ou R)
  - Anglais suivi à l'ENSIMAG (+ 2eme langue)
  - Validation REX (le 3/10 après-midi) / simulation gestion
  - Stage 2A à valider
  - Elective unit: NTC ou « smart card security »
  - *PFE + Thèse Master (juil pou R, sept pour P)*
- *Facultatifs: Sport, LV2, …*
- *Définir programme suivi: choix M2R ou choix M2P*

# Contacts and links

- Academic supervisors:
  - (UJF) Philippe Elbaz-Vincent Philippe.Elbaz-Vincent@ujf-grenoble.fr
  - (INP) Jean-Louis Roch Jean-Louis.Roch@imag.fr
- Administration: registration, timetable, …
  - UJF : Cécile Gros Cecile.Gros@ujf-grenoble.fr
  - INP / Ensimag: Elena Leibowitch Elena.Leibowitch@imag.fr

- Links
  - SCCI web server: http://scci.imag.fr
    - Kiosk: https://intranet.ensimag.fr/KIOSK/MasterCSCI/
    - Mail: scci@ensimag and m2scci.im2ag@ujf-grenoble.fr

# Timetable ADE : HowTo

**If you do not have an Agalan INP login+pwd :**

https://edt.grenoble-inp.fr/2014-2015/exterieur

**Or if you have an AGALAN login+pwd:**

- Direct access all Master courses in Grenoble

| | |
|---|---|
| UJF | http://ade52-ujf.grenet.fr/ |
| INP | https://edt.grenoble-inp.fr/ |

- M2R SCCI (lectures from mid-september to january) :
  copy-paste in your browser the url : with INP Agalan login+pwd:
  - **https://edt.grenoble-inp.fr/2014-2015/enseignant/*/jsp/custom/modules/plannings/direct_planning.jsp?resources=10108**
  - M2P SCCI (lectures from mid-september to march)
    copy-paste in your browser the url :
    https://edt.grenoble-inp.fr/2014-2015/enseignant/*/jsp/custom/modules/plannings/direct_planning.jsp?resources=10109

# Validation / Graduation

- Two semesters / periods
  - S3 (30 credits) : Courses
  - S4 (30 credits): Master thesis (internship) + English (or French)

- Each semester has to be validated :
  - Requirements for S3 validation :
    - In each module: global mark ≥  7/20 (35%)
    - Global average mark (GPA) on S3 ≥ 10/20 (50%)
  - Requirements for S4validation :
    - Master thesis mark ≥ 10/20 (50%)
    - English: B2 level (Alt or Full)

- IMPORTANT: **No compensation between semesters**
  - Except if the candidate has a GPA in S3 (courses)  ≥ 9.75 and no mark < 7 in some module

  - For honours: the Master degree includes the 4 semesters (M1 and M2)

# REGISTRATION

- Deadline 1st October
- BUT : As soon as possible !!!

  -
    ```
    If (registration == OK ) {
               Create_login() ;
              ADE_timetable_access,  Kiosk, ….
     }
    ```
  - Thus: While not registered:  no login, no Kiosk, no ADE,

# Important points

- **Registration**
- Individual interviews (current october)
- **Internship / Master Thesis**
  - Curriculum vitae ready
  - Prospection / application : from early October

# Other contacts

- **SECURIMAG club**

- **CELAIO :** Carole.Durand@ujf-grenoble.fr
  - Relations with companies
  - CV, internship contracts, …

- **International** : Cecile.Garatti@ujf-grenoble.fr
  ri.im2ag@ujf-grenoble.fr