Master 2 Cybersecurity

Cryptology & Security; Informatics & cyber-physical systems

UGA directors: **Jean-Guillaume Dumas, Vanessa Vitse**

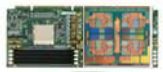
Ensimag director: **Jean-Louis Roch**

M2 CyberSecurity (CS)

1 year dedicated program at University Grenoble Alpes (UGA)

Ensimag + ufr IM²AG

cybersecurity.imag.fr



- **Goals**: formation of experts in security and coding technologies
  - **Cryptology**: mathematical protocols (RSA, AES, ECC, SHA3, PKI…)
  - **Security**: software/hardware (network, system, integration), audit
  - **Applications**: watermarking, multimedia, smartcard, …

- **M2 P+R** : Directed to research and profession
  - Sept.-Jan.: lectures+training
  - Jan.-Sept.: project/internship

CyberSecurity courses

Contents	Credits	Sem.
Software security, secure programming and **computer forensic**	3	S9
Security architectures : network, system, key managements, cybersecurity of industrial IT	6	S9
Cryptographic engineering, **protocols and security models**, data privacy, coding and applications	6	S9
Threat and risk analysis, IT security **audit** and norms	3	S9
Hardware and **embedded** systems **security**	6	S9
Optional: **Advanced Cryptology**	6	S9
Optional: **Advanced Security**		
Option: Informatique légale et **aspects juridiques**		
Internship (within a Company or in a research unit)	27	S10
Language (English mandatory B2 level)	3	Year

Research environment

- Cybersecurity: versatile domain, within different departments
  - LIG, LJK, Institut Fourier, Verimag, TIMA, GIPSA-Lab, Inria, CEA

  (all these Grenoble « labs » participate in the courses)

- Various aspects: complementary
  - Example: industrial contract ARAMIS [Atos World-Grid, 2014-2017]
  - Many research projects (French ANR, Europe, etc.)

- A Labex Persyval team
  - SCCyPHy « Security and Cryptology for CyberPhysical systems »
  - Co-Directors: Claude Castelluccia (INRIA), Jessy Clédière (CEA), Philippe Elbaz-Vincent (UGA), Régis Leveugle (INP)
  - Security activies in Grenoble

Following SCCI

- Security, Cryptology and Coding of Information
  - 2002 → 2016: about 500 students
- Becomes Cybersecurity
  - From 2016

Examples of Master thesis/PFE

- **Integration of zero-knowledge authentication on smart card** [C-S]
  - Secure server for SIP telecommunications [INRIA]
  - Integration of strong authentication in an information system [British Telecom]
  - Management of identity for printer access [Helwett-Packard, Germany]
  - Reconfiguraton of a secure infrastructure [France-Telecom, Grenoble]

- **Conception et réalisation d'un composant de sécurité** [Ministère Défense, Paris]
  - Analysis and deployment of a confidential data service [Solucom, Nantes]
  - Integration of biometrics in crypto protocols [SAGEM, Paris]

- **Hidden channel attacks** [SAGEM, Paris]
  - Windows CardSpace components in a smart card [Gemalto, La Ciotat]
  - Secure loading of jar in JavaCard3.0 [Gemalto, La Ciotat]
  - Lightweight electronic signature [Dictao, Paris]
  - Wireless infrastructure for emergency comm. [Wisecomm, Germany]
  - Secure and anonymous communication on internet [UL, Luxembourg]
  - Test of crypto-secure random generators [LTSI, Lyon]

- **Security analysis of a medical data protection scheme [Philips, Eindhoven]**
  - Supervision of the CEA computer infrastructure [CEA, Grenoble]
  - Security analysis of images watermarking [GIPSA, Grenoble]
  - Security audit of the SCADA platform [Atos Origin, Grenoble]

Partners

- Thales
- Actoll
- ST Micro
- Amadeus
- Sopra group
- Logica
- Solucom
- Accenture
- C-S
- EADS
- Technicolor
- CEA LETI
- Xerox
- Tiempo
- Orange Labs (Caen, Grenoble)
- Netheos
- Medasys infrastructure
- Police scientifique
- Oberthur
- Cap Gemini
- Schneider Electric
- Canal+ Technologies (Nagra)
- Netasq SA
- Aatlantide
- Gemalto
- Banque de France
- Atos
- SFR
- Onix
- Edelweb
- Aliantiz
- Caisse d'épargne
- Motorola
- Laboratoires CNRS, INRIA, Universities

…

Examples of PhD

- **Sébastien Varrette**
  - 2003: M2 SCCI
  - 2003-2007: Thèse à Grenoble (LIG-Inria [Roch]) et Univ. Luxembourg [Leprévost]
  - **Security in Large Scale Distributed Systems: Authentication and Result Checking**
  - Since 2007: **Research fellow Université Luxembourg** [Distributed Platforms Security and HPC systems]
- **Alexandre Berzati**
  - 2007: M2 SCCI
  - 2007-2010: Thèse CEA Grenoble [Dumas] – UVSQ Versailles [Goubin]
  - **Analyse cryptographique des altérations d'algorithmes**
  - 2010: Postdoc CEA Cadarache
  - Since 2011: **Engineer expert INVIA** [Semiconductor design for embedded security]
- **Thomas Roche**
  - 2006: M2 SCCI
  - 2007-2010: Thèse à Grenoble (LIG [Roch] – IF [Gillard]) - CIFRE (C-S Paris)
  - **Dimensionnement et intégration d'un chiffre symétrique (…)**
  - 2010-2011: Postdoc Paris-8
  - Since 2011: **ANSSI** (Agence nationale de la sécurité des systèmes d'information) , then **APPLE**
- Also

J. Javelle (LIG), M.-A. Cornelie (IF), A. Kumar (Inria/LIG/Verimag), M. Duclos (Verimag, 2016), K. Layat (IF, 2015), Z. Sultan (LIG/LJK, 2016), G. Dejulis (IF, 2014), R. Jamet (Verimag, 2015), M-A Cornelie (IF 2016), J-B Orfila (LJK), E. Perrier (LIG), M. Puys (Vérimag), …

cybersecurity.imag.fr

- ADE: planning
- Calendar: Sept. Jan. + vacations
- Regulations (in French):
  - Course = 50% Exam + 50% Practice/Interrogations
  - Practice /Interrogations mandatory (ABJ 0/20, ABI DEF)
  - Average $\geq$ 10/20, for each semester
  - No course below 7/20
  - English B2
  - Internship: 4 to 6 months
  - …

Master 2 = Semesters 9 & 10

- Semester 9: 14 weeks
  - Part 1: 7 weeks from Sept. 19 to Nov. 10
  - Part 2: 7 weeks from Nov. 15 to Jan. 13
    - Optional courses: choice before Sept 30th 2016.
- Exams: Jan 23 – 27, 2017
  - 2nd session: June 19 – 23, 2017
- Semester 10: Internship
  - Internship defenses: September 4 – 8, 2017

September 19 – November 10

7 weeks: from September 19 to November 10
vacances toussaint ; Friday November 11, vacation;
Thursday October 13, FEEL

		Monday	Tuesday	Wednesday	Thursday	Friday
3h+1.5h Morning	8h00-9h30 & 9h45-11h15	GBCY9U04 Risk Analysis	RATTRAPAGE GBCY9U02 Security Arch.	GBCY9U05 Embedded Sec.	GBCY9U03 Crypto Eng.	GBCY9U03 Crypto Eng.
	11h30-13h00	RATTRAPAGE	GBCY9U01 Software Security	GBCY9U05 Embedded Sec.	RATTRAPAGE	GBCY9U03 Crypto Eng.
3h Afternoon	13h45-15h15 & 15h30-17h00	GBCY9U02 Security Arch.	Anglais	GBCY9U01 Software Security GBCY9U02 Security Arch.	conférences industrielles + RATTRAPAGE	GBCY9U05 Embedded Sec.

November 15 – January 6

6 weeks : November 15 to January 6 ;
November 18 GreHack ;
Monday January 2, vacation

		Monday	Tuesday	Wednesday	Thursday	Friday
3h+1.5h Morning	8h00-9h30 & 9h45-11h15	OPTION: -/Advanced Crypto. -/Advanced Secu. -/Info. Légale	OPTION: -/Advanced Crypto. -/Advanced Secu. -/Info. Légale	GBCY9U05 Embedded Sec.	GBCY9U01 Software Security	GBCY9U03 Crypto Eng.
	11h30-13h00	Info Légale	Info Légale	GBCY9U05 Embedded Sec.	RATTRAPAGE	GBCY9U03 Crypto Eng.
3h Afternoon	13h45-15h15 & 15h30-17h00	GBCY9U02 Security Arch.	Anglais	GBCY9U02 Security Arch.	conférences industrielles + RATTRAPAGE	GBCY9U04 Risk Analysis

January 9 – January 13

1 week: January 9 – January 13

		Monday	Tuesday	Wednesday	Thursday	Friday
3h+1.5h Morning	8h00-9h30 & 9h45-11h15	OPTION: -/Advanced Crypto. -/Advanced Secu. -/Info. Légale	OPTION: -/Advanced Crypto. -/Advanced Secu. -/Info. Légale	GBCY9U05 Embedded Sec.	GBCY9U03 Crypto Eng.	GBCY9U03 Crypto Eng.
	11h30-13h00	Info Légale	Info Légale	GBCY9U05 Embedded Sec.	Info Légale	GBCY9U03 Crypto Eng.
3h Afternoon	13h45-15h15 & 15h30-17h00	GBCY9U02 Security Arch.	GBCY9U04 Risk Analysis	GBCY9U03 Crypto Eng.	conférences industrielles + RATTRAPAGE	GBCY9U04 Risk Analysis

Optional courses

- Advanced Cryptology
  - Vanessa Vitse
- Advanced Security
  - Cédric Lauradoux
- Informatique Légale
  - Philippe Elbaz-Vincent

UGA / INP

- Thursday 22nd September
  - Registration

- English
  - UGA
  - INP