Master 2 Cybersecurity

Cryptology & Security; Informatics & cyber-physical systems

UGA director: **Clément PERNET**
Ensimag director: **Marie-Laure POTET**

http://cybersecurity.imag.fr

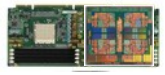
September 21, 2020

M2 CyberSecurity (CS)

1 year dedicated program at Université Grenoble Alpes (UGA)

Ensimag + UFR IM²AG

cybersecurity.imag.fr application from Jan. (FSA)



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

- **M2 P+R** : Directed to Research and Industry
  - Sept.-Jan.: lectures + training
  - Feb.-Sept.: project / internship

CyberSecurity courses

Contents	Credits	Sem.
Software security, secure programming and computer forensic	3	S9
Security architectures : network, system, key managements, blockchains, 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
Group: **Advanced Cryptology**	6	S9
Group: **Advanced Security**		
Internship (within a Company or in a research unit)	30	S10

Research environment

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

  (all these Grenoble research units « labs » are involved in the courses)

- Complementary aspects:
  - Academia + Industry + Government
  - Example: industrial contract ARAMIS [Atos World-Grid, 2014-2017]
  - Many research projects (French ANR, MinDef, Europe, etc.)

- An Idex project « Grenoble Alpes Cybersecurity Institute »
  - Federate Security activities in Grenoble between science
  - and humanities

Cybersecurity Institute
Univ. Grenoble Alpes

An already long history

- Security, Cryptology and Coding of Information Master
  - 2002 - 2016: about 400 students
- Becomes Cybersecurity in 2016
- Total over 500 graduates ...

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]

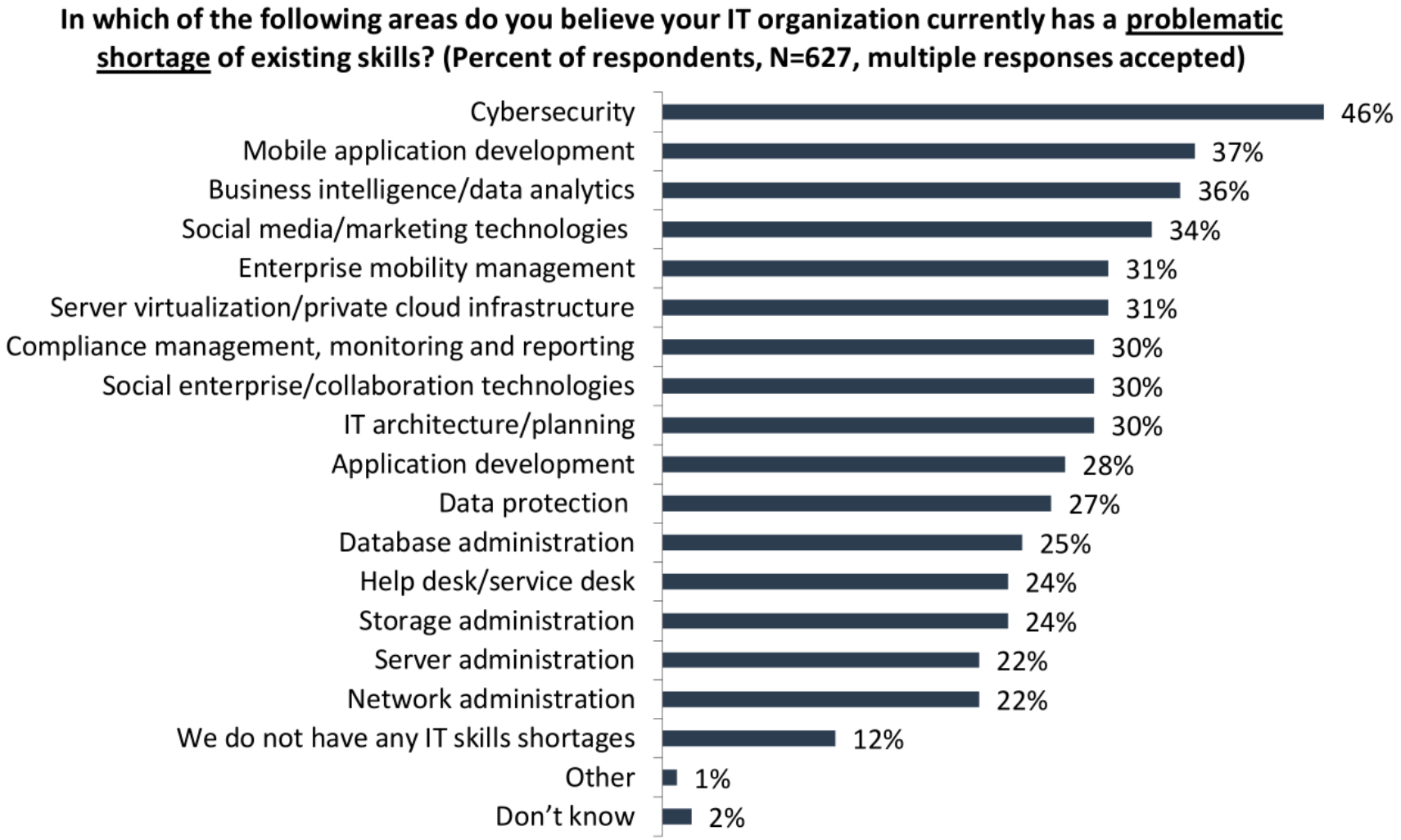
- **Hidden channel attacks** [SAGEM, Paris]
- Windows CardSpace components in a smart card [Gemalto, La Ciotat]
- Secure loading of jar in JavaCard3.0 [Gemalto, La Ciotat]
- Lightweight electronic signature [Dictao, Paris]
- Wireless infrastructure for emergency comm. [Wisecomm, Germany]
- Secure and 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
- Ernst & Young
- ST Micro
- Amadeus
- Sopra group
- Logica
- Solucom
- Accenture
- MinDef
- Tessi lab
- C-S
- EADS
- Technicolor
- CEA LETI
- Xerox
- Tiempo
- Orange Labs (Caen, Arcueil, Rennes, Paris, Grenoble)
- Netheos
- Medasys infrastructure
- CGI
- Sogeti High Tech
- Mathworks
- Consensys
- Deloitte
- Police scientifique
- Oberthur
- Cap Gemini
- Schneider Electric
- Canal+ Technologies (Nagra)
- Netasq SA
- Aatlantide
- Gemalto
- Banque de France
- Atos
- SFR
- Onix
- Edelweb
- Prowebce
- Microstore
- Aliantiz
- Airbus
- DCNS
- Caisse d’épargne
- Motorola
- Laboratoires CNRS, INRIA, Universities
- …

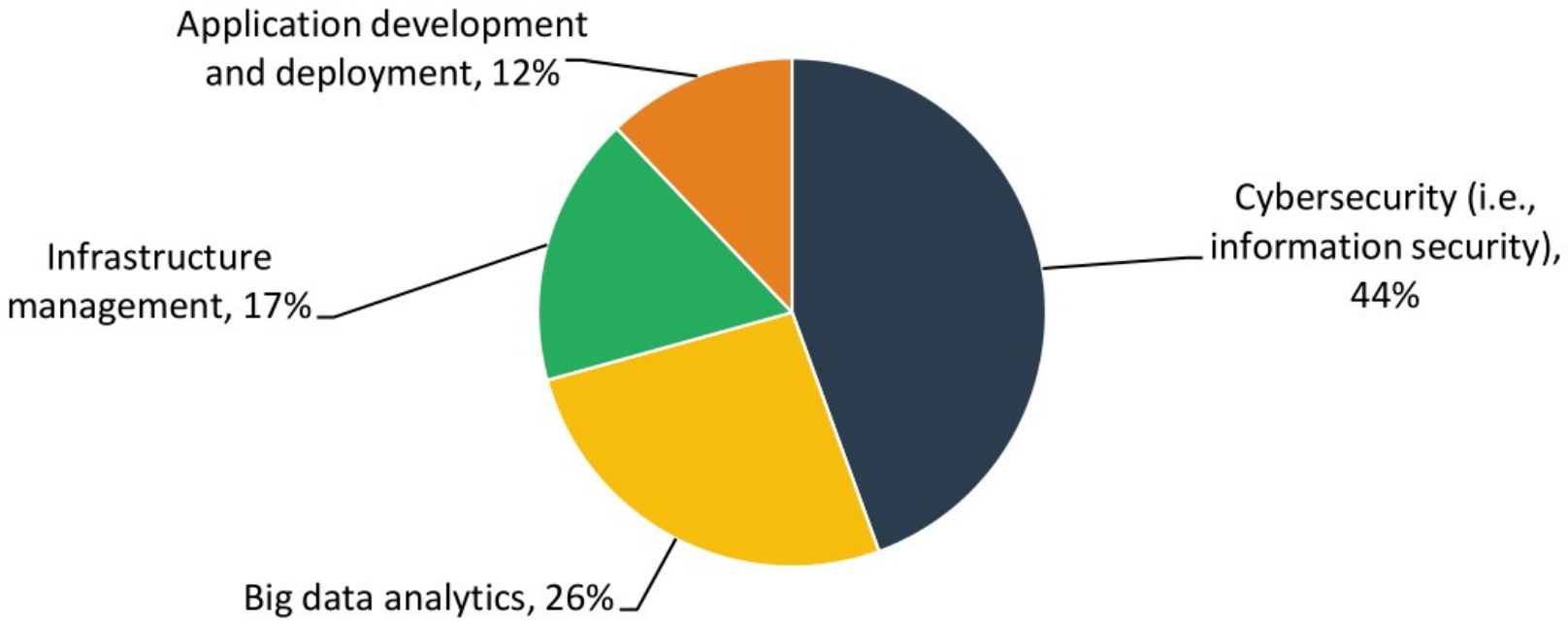
IT skills shortage



Source: Enterprise Strategy Group, 2016.

Career growth potential

In which of the following functional areas do you believe skills development would be most beneficial to your employees (i.e., IT staff) in terms of their career path and benefit to your organization? (Percent of respondents, N=627)



Source: Enterprise Strategy Group, 2016.

Examples of PhD

- **Nicolas Bordes**

  2017: M2 CyberSecurity

  2018-20...: PhD Grenoble LJK [Karpman, Dumas]

  Symmetric primitives of low multiplicative complexity, side channel attacks and masking

- **Alexandre Berzati**

  2007: M2 SCCI

  2007-2010: PhD 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: PhD 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), J-B Orfila (LJK 2018), M. Puys (Vérimag 2017),

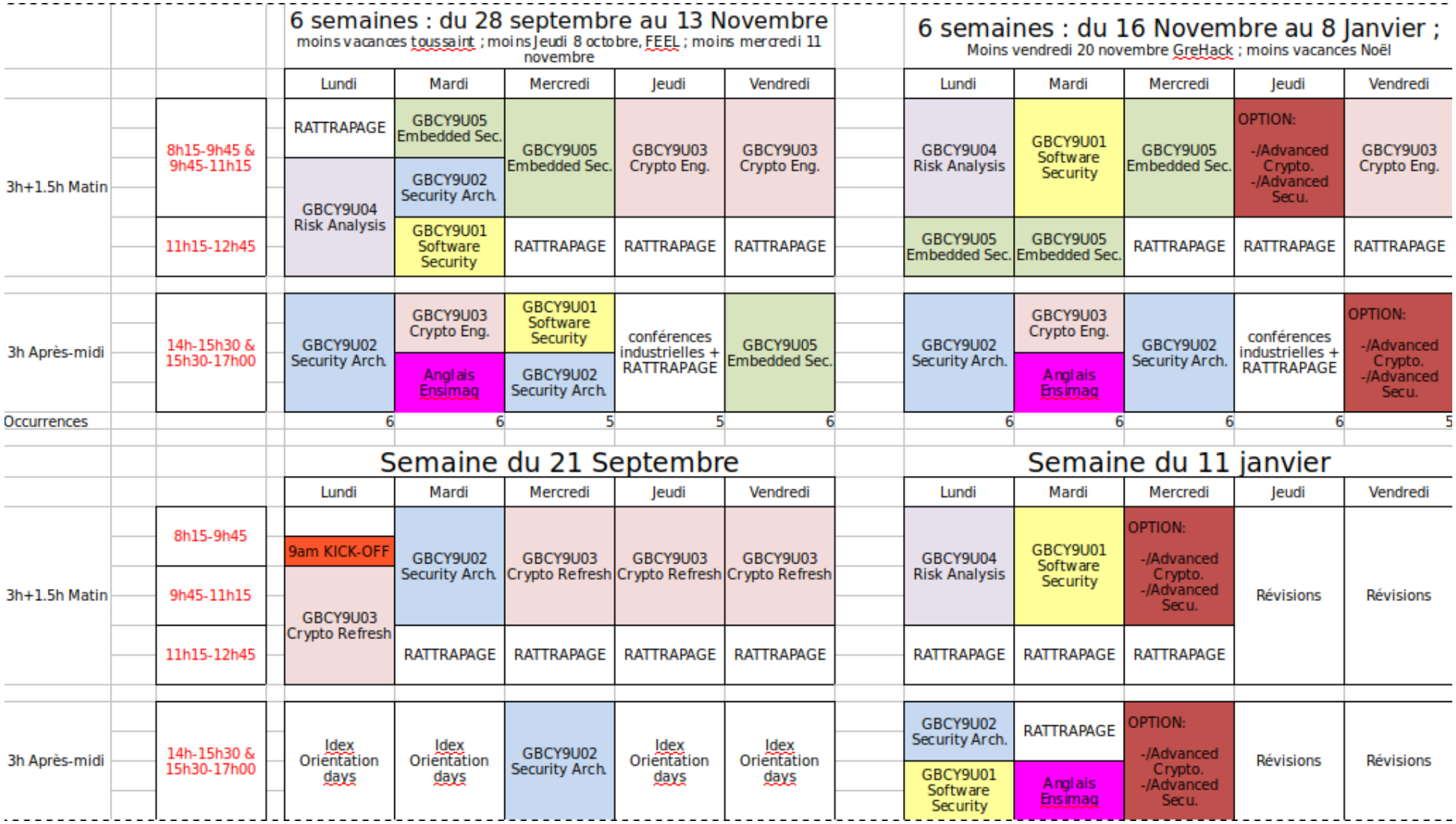
cybersecurity.imag.fr

- ADE: planning
- Calendar: Sept. - Jan. + holidays
- Regulations (in French):
  - Course ≈ 50% Exam + 50% Practice/Interrogations
  - Practice / Interrogations mandatory (ABJ 0/20, ABI DEF)
  - Average 10/20, for each semester
  - No course below 7/20
  - FLE (Français langue étrangère) is proposed
  - Internship: 5 to 6 months
- Jury, diploma : Sept. 2021.

Master 2 = Semesters 9 & 10

- Welcome week: Sept. 16 to 18, 2020
  - Foreign students welcome, administrative registration, training
- Semester 9: 14 weeks
  - Part 1: 7 weeks from Sept. 21 to Nov. 13 (first week refresh)
  - Part 2: 7 weeks from Nov. 16 to Jan. 15 (group option start, last week = catch-up slots)
- Exams: **Jan 18 – 22, 2021**
  - 2nd session: April 2021
- Semester 10: Internship
  - Internship defenses: September 1 – Sept. 6, 2021
  - ⇨Start now to look for one

Semester 9: 14 weeks



		6 semaines : du 28 septembre au 13 Novembre moins vacances toussaint ; moins Jeudi 8 octobre, FEEL ; moins mercredi 11 novembre				
		Lundi	Mardi	Mercredi	Jeudi	Vendredi
3h+1.5h Matin	8h15-9h45 & 9h45-11h15	RATTRAPAGE	GBCY9U05 Embedded Sec.	GBCY9U05 Embedded Sec.	GBCY9U03 Crypto Eng.	GBCY9U03 Crypto Eng.
		GBCY9U04 Risk Analysis	GBCY9U02 Security Arch.			
	11h15-12h45		GBCY9U01 Software Security	RATTRAPAGE	RATTRAPAGE	RATTRAPAGE
3h Après-midi	14h-15h30 & 15h30-17h00	GBCY9U02 Security Arch.	GBCY9U03 Crypto Eng.	GBCY9U01 Software Security	conférences industrielles + RATTRAPAGE	GBCY9U05 Embedded Sec.
			Anglais Ensimag	GBCY9U02 Security Arch.		
Occurrences		6	6	5	5	6

		6 semaines : du 16 Novembre au 8 Janvier ; Moins vendredi 20 novembre GreHack ; moins vacances Noël				
		Lundi	Mardi	Mercredi	Jeudi	Vendredi
3h+1.5h Matin	8h15-9h45 & 9h45-11h15	GBCY9U04 Risk Analysis	GBCY9U01 Software Security	GBCY9U05 Embedded Sec.	OPTION: -/Advanced Crypto. -/Advanced Secu.	GBCY9U03 Crypto Eng.
	11h15-12h45	GBCY9U05 Embedded Sec.	GBCY9U05 Embedded Sec.	RATTRAPAGE	RATTRAPAGE	RATTRAPAGE
3h Après-midi	14h-15h30 & 15h30-17h00	GBCY9U02 Security Arch.	GBCY9U03 Crypto Eng.	GBCY9U02 Security Arch.	conférences industrielles + RATTRAPAGE	OPTION: -/Advanced Crypto. -/Advanced Secu.
			Anglais Ensimag			
Occurrences		6	6	6	6	5

		Semaine du 21 Septembre				
		Lundi	Mardi	Mercredi	Jeudi	Vendredi
3h+1.5h Matin	8h15-9h45	9am KICK-OFF	GBCY9U02 Security Arch.	GBCY9U03 Crypto Refresh	GBCY9U03 Crypto Refresh	GBCY9U03 Crypto Refresh
	9h45-11h15	GBCY9U03 Crypto Refresh				
	11h15-12h45		RATTRAPAGE	RATTRAPAGE	RATTRAPAGE	RATTRAPAGE
3h Après-midi	14h-15h30 & 15h30-17h00	Idex Orientation days	Idex Orientation days	GBCY9U02 Security Arch.	Idex Orientation days	Idex Orientation days

		Semaine du 11 janvier				
		Lundi	Mardi	Mercredi	Jeudi	Vendredi
3h+1.5h Matin	8h15-9h45 & 9h45-11h15	GBCY9U04 Risk Analysis	GBCY9U01 Software Security	OPTION: -/Advanced Crypto. -/Advanced Secu.	Révisions	Révisions
	11h15-12h45	RATTRAPAGE	RATTRAPAGE	RATTRAPAGE		
3h Après-midi	14h-15h30 & 15h30-17h00	GBCY9U02 Security Arch.	RATTRAPAGE	OPTION: -/Advanced Crypto. -/Advanced Secu.	Révisions	Révisions
		GBCY9U01 Software Security	Anglais Ensimag			

Advanced Cryptology/Security

- Course with choice
- Starts November 21st 2020

Pierre Karpman / Cédric Lauradoux

- Shared Plenary courses (CM)
- Elective lab (TP) and practical sessions (TD)

Some Events

- FEEL: **Thursday Oct. 8th, 2020**
- GreHack 2020: **Friday Nov. 20th, 2020**
  - https://grehack.fr
- Forum Emploi-maths (Paris): **Oct. 20th, 2020**
- Forum int. de la Cybersécurité: **Jan 19-21th, 2021**
  - www.forum-fic.com (Lille)

Registrations

- From **Wednesday September 16th, 2020**
  - Registration UGA / INP
  - Use your **@univ-grenoble-alpes.fr** and **@grenoble-inp.org** addresses

- Master mention, choice of:
  - Informatique (Computer science)
  - Mathématiques & applications