PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

NEW

ENGINEER SPECIALIZATION PROGRAM OFFER (ACADEMIC)

(FROM 3RD YEAR TO 5TH YEAR)

Establishment	Faculty	Department

Domain	Sector	Specialty
Mathematics, and Computer Sciences	**Computer Sciences**	**Computer Security**

Academic Year: 2024-2025.

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جديد

عرض تكوين مهندس تخصصي
(أكاديمي)
(من السنة الثالثة إلى السنة الخامسة)

المؤسسة	الكلية	القسم

الميدان	الشعبة	التخصص
رياضيات و إعلام آلي	إعلام آلي	أمن المعلوماتية

السنة الجامعية: 2025/2024.

SUMMARY

I – Engineering Identity Card.

1 – Course Location.

Faculty:

Department:

2- Course Partners[1].

- Other University Establishments:

- Businesses and Other Socio-Economic Partners:

- International Partners:

3- Context and Objectives of the Course.

A- Access Conditions.

B- Course Objectives.

C- Targeted Profiles and Skills.

[1] Present the Conventions as an Appendix to the Offer.

D- Regional and National Employability Potential.

E- Gateways to Other Specialties.

F- Course Monitoring Indicators.

G- Supervisory Abilities. (Give the Number of Students that it's Possible to Support).

The Supervision Capacity is Estimated at **……**.

4- Human Resources Available.

A- Teaching Staff in the Specialty.

First, and last name	Diploma	Degree	Laboratory	Specialty	Intervention Type [2]	Signature

[2] Course, Directed Work, Practical Work, Internship Supervision, Supervision, Co-Supervision, and Other.

First, and last name	Diploma	Degree	Laboratory	Specialty	Intervention Type [3]	Signature

[3] Course, Directed Work, Practical Work, Internship Supervision, Supervision, Co-Supervision, and Other.

B- External Supervision.

Affiliation Establishment.

First, and last name	Diploma	Degree	Laboratory	Specialty	Intervention Type [4]	Signature

Affiliation Establishment.

First, and last name	Diploma	Degree	Laboratory	Specialty	Intervention Type	Signature

Affiliation Establishment.

First, and last name	Diploma	Degree	Laboratory	Specialty	Intervention Type	Signature

[4] Course, Directed Work, Practical Work, Internship Supervision, Supervision, Co-Supervision, and Other.

5- Specific Available Material Means.

A- Pedagogical Laboratories and Equipment.

Laboratory Title: **Practical Work Room No. 01.**

N°	Equipment Title	Number	Observations

Laboratory Title: **Practical Work Room No. 02.**

N°	Equipment Title	Number	Observations

B- Internship Sites and In-Company Training.

Internship Location	Number of Students	Internship Duration

C- Research Laboratory Supporting the Course.

Laboratory Head:
Approval Number:
Date: **Opinion of the Laboratory Head:** **Avis Favorable.**

D- Research Projects Supporting the Course.

Project Title	Project Code	Project Start Date	Project End Date

E- Personal Work Areas and ICT.

II- Program Semester Organization Sheet.

1- Semester 5.

Teaching Unit	H-YHV[5]	Weekly HV[6]				Coeff.	Credits	Evaluation Modes	
	14 Weeks	Course	DW[7]	PW[8]	Personal Work			Continuous	Exam
Fundamental Teaching Unit (FTU)									
FTU51:	**126h**	**3h**	**3h**	**3h**	**6h**	**6**	**10**		
Mathematics Tools for Cryptography		1h30	1h30	1h30	3h	4	6	50%	50%
Operational Research		1h30	1h30	1h30	3h	2	4	50%	50%
FTU52:	**105h**	**3h**	**3h**	**1h30**	**6h**	**5**	**10**		
Compilation		1h30	1h30	1h30	3h	3	6	50%	50%
Software Engineering		1h30	1h30		3h	2	4	40%	60%
Methodological Teaching Unit (MTU)									
MTU5:	**84h**	**3h**		**3h**	**6h**	**4**	**7**		
Advanced Programming		1h30		1h30	3h	2	4	40%	60%
Web Development		1h30		1h30	3h	2	3	40%	60%
Discovery Teaching Unit (DTU)									
DTU5:	**42h**	**1h30**	**1h30**		**3h**	**1**	**2**		
Theory of Information and Coding		1h30	1h30		3h	1	2		100%
Transversal Teaching Unit (TTU)									
TTU5:	**21h**	**1h30**			**3h**	**1**	**1**		
Business Intelligence		1h30			3h	1	1		100%
Total Semester 5	**378h**	**12h**	**7h30**	**7h30**	**24h**	**17**	**30**		

[5] Half-Yearly Hourly Volume.
[6] Weekly Hourly Volume.
[7] Directed Work.
[8] Practical Work.

2- Semester 6.

Teaching Unit	H-YHV	Weekly HV				Coeff.	Credits	Evaluation Modes	
	14 Weeks	Course	DW	PW	Personal Work			Continuous	Exam
Fundamental Teaching Unit (FTU)									
FTU61:	**126h**	**3h**	**3h**	**3h**	**6h**	**7**	**12**		
Advanced Cryptography		1h30	1h30	1h30	3h	4	6	50%	50%
Modeling and Simulation		1h30	1h30	1h30	3h	3	6	50%	50%
FTU62:	**105h**	**3h**	**1h30**	**3h**	**6h**	**4**	**8**		
Cloud Computing		1h30		1h30	3h	2	4	40%	60%
Advanced Databases		1h30	1h30	1h30	3h	2	4	50%	50%
Methodological Teaching Unit (MTU)									
MTU6:	**84h**	**3h**	**1h30**	**1h30**	**6h**	**4**	**7**		
Mobile Development		1h30		1h30	3h	2	3	40%	60%
Digital Signal Processing		1h30	1h30	1h30	3h	2	4	50%	50%
Discovery Teaching Unit (DTU)									
DTU6:	**42h**	**1h30**	**1h30**		**3h**	**1**	**2**		
AI Notions and Principles		1h30	1h30		3h	1	2	40%	60%
Transversal Teaching Unit (TTU)									
TTU6:	**21h**	**1h30**			**3h**	**1**	**1**		
Startup and Professional Development		1h30			3h	1	1		100%
Total Semester 6	**378h**	**12h**	**7h30**	**7h30**	**24h**	**17**	**30**		

3- Semester 7.

Teaching Unit	H-YHV	Weekly HV				Coeff.	Credits	Evaluation Modes	
	14 Weeks	Course	DW	PW	Personal Work			Continuous	Exam
Fundamental Teaching Unit (FTU)									
FTU71:	**126h**	**4h30**	**1h30**	**3h**	**3h**	**6**	**10**		
Advanced Operating Systems		1h30		1h30	3h	3	5	40%	60%
Advanced Networks		3h	1h30	1h30		3	5	50%	50%
FTU72:	**105h**	**3h**		**4h30**	**6h**	**4**	**10**	40%	60%
Computer Systems Security		1h30		3h00	3h	2	5	40%	60%
Information and Data Security		1h30		1h30	3h	2	5	40%	60%
Methodological Teaching Unit (MTU)									
MTU7:	**84h**	**3h**	**1h30**	**1h30**	**6h**	**4**	**7**		
Programming by Constraint		1h30	1h30		3h	2	3	40%	60%
Machine Learning, Deep Learning, and Security		1h30		1h30	3h	2	4	40%	60%
Discovery Teaching Unit (DTU)									
DTU7:	**42h**	**1h30**		**1h30**	**3h**	**2**	**2**		
Malwares Analysis		1h30		1h30	3h	2	2	40%	60%
Transversal Teaching Unit (TTU)									
TTU7:	**21h**	**1h30**			**1h30**	**1**	**1**		
Critical Thinking and Creativity Skills		1h30			1h30	1	1		100%
Total Semester 7	**378h**	**13h30**	**3h**	**10h30**	**19h30**	**17**	**30**		

4- Semester 8.

Teaching Units	H-YHV	Weekly HV				Coeff.	Credits	Evaluation Modes	
	14 Weeeks	Course	DW	PW	Personal Work			Continuous	Exam
Fundamental Teaching Unit (FTU)									
FTU81:	**84h**	**3h**		**3h**	**6h**	**5**	**10**		
Operating System Security		1h30		1h30	3h	2	5	40%	60%
Cybersecurity		1h30		1h30	3h	3	5	40%	60%
FTU82:	**126h**	**3h**	**1h30**	**4h30**	**6h**	**5**	**10**		
Network Security		1h30	1h30	1h30	3h	3	5	50%	50%
Wireless and Mobile Network Security		1h30		3h00	3h	2	5	40%	60%
Methodological Teaching Unit (MTU)									
MTU8:	**105h**	**3h**	**1h30**	**3h**	**6h**	**3**	**6**		
Identity & Access Management		1h30		1h30	3h	1	2	40%	60%
Secure Software Development		1h30	1h30	1h30	3h	2	4	50%	50%
Discovery Teaching Unit (DTU)									
DTU8:	**21h**	**1h30**			**3h**	**1**	**1**		
Innovation and Entrepreneurship		1h30			3h	1	1		100%
Transversal Teaching Unit (TTU)									
TTU8:	**42h**			**3h**	**3h**	**3**	**3**		
Multidisciplinary Project				3h	3h	3	3		100%
Total Semester 8	**378h**	**10h30**	**3h**	**13h30**	**21h**	**17**	**30**		

5- Semester 9.

Teaching Units	H-YHV	Weekly HV				Coeff.	Credits	Evaluation Modes	
	14 Weeks	Course	DW	PW	Personal Work			Continuous	Exam
Fundamental Teaching Unit (FTU)									
FTU9:	**126**	**4h30**		**4h30**	**9h**	**10**	**18**		
Web and mobile application security		1h30		1h30	3h	3	6	40%	60%
Emblemed Systems Security		1h30		1h30	3h	4	6	40%	60%
Digital Forensics		1h30		1h30	3h	3	6	40%	60%
Methodological Teaching Unit (MTU)									
MTU9:	**84h**	**3h**		**3h**	**6h**	**5**	**9**		
DevOps		1h30		1h30	3h	3	5	40%	60%
Hacking Ethic		1h30		1h30	3h	2	4	40%	60%
Discovery Teaching Unit (DTU)									
DTU9:	**63h**	**3h**	**1h30**		**3h**	**1**	**2**		
Project Management		1h30	1h30		3h	1	1	40%	60%
Emerging Security Technologies		1h30			3h	1	1		100%
Transversal Teaching Unit (TTU)									
TTU9:	**21h**	**1h30**			**3h**	**1**	**1**		
Academic Communication and Research		1h30			3h	1	1		100%
Total Semester 9	**294h**	**10h30**	**1h30**	**7h30**	**21h**	**17**	**30**		

6- Semester 10

Domain **:** Mathematics and Computer Science.
Sector **:** Computer Science.
Specialty **:** Computer Security

The S10 Semester is Reserved for the Final project, culminated by a deliverable, dissertation and a defense.

	HVS	Coeff.	Credit
Personal Work			
Internship In Company			
Seminars	125h	06	10
Other (Dissertation)	250h	11	20
Total Semester 10	**375h**	**17**	**30**

7- Course Overall Summary

LU / HV	FLU	MLU	DLU	TLU	Total
Course	420h	210h	84h	105h	819h
DW	189h	63h	42h	-	294h
PW	420h	168h	63h	-	651h
Personal Work	756h	420h	147h	189h	1512h
Semester 10	250h	125h	-	-	375h
Total	**2035h**	**986h**	**336h**	**294h**	**3671h**
Credits	128	36	11	5	**180**
% in Credits for Each LU	71.11%	20%	6.11	2.78	100%

III – Detailed Content by Subject.

Engineering Title: Computer Security.
Semester: 05.
TU Title:
Subject Title: Mathematics Tools for Cryptography.
Credits: 06.
Coefficient: 04.

Teaching Objectives: The first part introduces fundamental notions for group theory, notions useful for understanding bodies and linear codes as well as their applications. The second part should allow the student to acquire the elementary knowledge provided by the theory of finite bodies.

Recommended Prior Knowledge: Some algebra concepts.

Course Content:

Part 1.

1. Groups, examples.
2. Homomorphisms.
3. Subgroups, distinguished subgroups and quotient groups.
4. Cyclic groups, order of elements, index of a subgroup.
5. Center, centralizer, conjugation.
6. Special groups.
7. Permutation groups, matrix groups.
8. Examples of applications in cryptography.

Part 2.

1. Definitions, characteristics, cardinality of a finite field.
2. Frobenuis relation, Frobenuis morphism.
3. Construction and uniqueness of finite bodies, practical construction of Fq.
4. Sub field of a finite field, primitive element, primitive polynomial.
5. Irreducible polynomials and conjugate elements.
6. Factorization of x^(n) -1)
7. Congruences and Residual Classes.
8. Euler's Phi function, the Theorems of Fermat, Euler and Lagrange.
9. Quadratic residue.
10. Recurrent sequences and shift register.
11. Application examples: cryptographic keys.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. J. Querre, Cours d'algèbre, Maitrise de Mathématiques, Masson. 1976.
2. J. Calais. Éléments de théorie des groupes. PUF, 1998.
3. E. Ramis, C. Deschamps, et J. Odoux. Cours de Mathématiques 1, Algèbre. Dunod, 1998.
4. D.J.S. Robinson, "A course in the Theory of Groups," 2nd ed., Springer-Verlag, New York, 1995.
5. Rudolf Lid land Harald Niederreiter, Finite fields, Encyclopedia of Mathematics and applications, Cambridge University press, 1997.
6. M. Demazure. Cours d'algèbre. Primalité, divisibilité, codes. Cassini, 1997.

Engineering Title: Computer Security.
Semester: 05.
TU Title:
Subject Title: Operational Research.
Credits: 04.
Coefficient: 02.

Teaching Objectives: To introduce the student to representing a problem, gathering data and providing answers.

Recommended Prior Knowledge: Basic notions of mathematics.

Course Content:

I. Optimization in operational research.
- Model: represent a problem.
- Instantiate: gather data.
- Solve: provide an answer.
- Examination of some situations.

II. Linear programming in continuous variables.
- Formulations.
- Geometric properties.
- Simplex algorithms.
- Duality.
- Additional differences.

III. Linear programming in integer and mixed variables.
- Formulations.
- Relaxations.
- Easily solvable problems, total unimodularity.
- Branch and bound method.
- Situations mixing continuous variables and integer variables.
- Reference combinatorial optimization problem.

IV. Local optimization.
- Constraint-free optimization (optimal conditions, linear search methods, etc.).
- Optimization with constraint (optimal conditions, quadratic sequential programming, etc.).

V. Graphs theory.
- Become familiar with the basic terminology of graph theory.
- Discover how to represent graphs in computer memory.
- Examine and implement various graph traversal algorithms.
- Learn how to implement a shortest path algorithm.
- Examine and implement the minimum spanning tree algorithm.
- Explore topological sort.
- Learn how to find Euler circuits in a graph.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. D. de Werra, and T. M Liebling, Operational Research for engineers, polytechnic presses, 2003.
2. J-M. Hélary, and R. Pédrono, Operational Research: Guided Work, Hermann, 1983.
3. Y.Nobert, and R.Ouellet, Operational Research (3rd edition), Gaëtan Morin, 2002.

Engineering Title: Computer Security.
Semester: 05.
TU Title:
Subject Title: Compilation.
Credits: 6.
Coefficient: 3.

Teaching Objectives: The student will be able to differentiate between compiler and interpreter, the different phases of compilation, until the generation of the final code.

Recommended Prior Knowledge: Programming, and Language Theory.

Course Content:

I. Introduction to compilation.
- The different stages of compilation.
- Compilation, interpretation and translation.

II. Lexical analysis.
- Regular expressions.
- Grammars.
- Finite step automata.
- An example of a lexical analyzer generator: LEX.

III. Syntactic analysis.
- Definitions: Syntactic grammar, left recursion, left factorization, free grammar.
- Calculation of the sets of first and following.
- Descending analysis methods: Recursive descent, LL (1).
- Bottom-up analysis methods: LR (1), SLR (1), LALR (1), item method.
- An example of a parser generator: YACC.

IV. Syntax-driven translation.

V. Intermediate forms.
- Post fixed shape
- Quadruplets.
- Direct and indirect triplets.
- Abstract tree.

VI. Allocation - Substitution - Organization of data at runtime.

VII. Object Code Optimization.

VIII. Object Code Generation.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Alfred Aho, Ravi Sethi, Compilateurs : Principes, techniques et outils – Cours et exercices -, DUNOD 2000.
2. Benjamin Cummings, A Retargetable Compiler: Design and implementation, Addison Wesley 1995.

Engineering Title: Computer Security.
Semester: 05.
TU Title:
Subject Title: Software Engineering.
Credits: 4.
Coefficient: 2.

Teaching Objectives: To learn how to apply an analysis and design methodology for software development. In particular, to learn object modelling using the universal UML language.

Recommended Prior Knowledge: Algorithms, Information Systems, Object-Oriented Programming.

Course Content:

Chapter I. Introduction to Software Engineering.

1. Definitions and objectives.
2. Principles of Software Engineering.
3. Expected qualities of software.
4. Software life cycle.
5. Software lifecycle models.

Chapter II. Information System design methods.

1. The challenges of the systems approach.
2. Concept of a system.
3. Typology of systems.
4. System design methods.
   - 4.1 Static system design.
     - 4.1.1 STB.
     - 4.1.2 SADT method.
     - 4.1.3 Entity Association Model.
   - 4.2 Dynamic system design.
     - 4.2.1 Prototyping.
     - 4.2.2 Object-oriented approaches.

Chapter III. Modelling with UML.

1. Introduction (Modelling, Model, Object Oriented Modelling, UML in application.).
2. General elements and mechanisms.
3. UML views and diagrams.
4. Packages.

Chapter IV. UML: Functional view & Static view.

1. Use case diagram.
2. Class diagram.
3. Object diagram.

Chapter V. UML: Dynamic view.

1. Interaction diagram (Sequence and collaboration).
2. Activity diagram.
3. State/transition diagram.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. - Pierre Gérard, Génie Logiciel : Principes et Techniques. Un cours pour Licence Pro, Université de Paris 13 LIPN. FC 2007/2008.
2. - Yann-Gaël Guéhéneuc, Gestion de projet pour le développement et la maintenance des logiciels. Cours au Département d'informatique et de recherche opérationnelle, Université de Montréal, Canada, 2003.
3. - Yende Raphael Grevisse, Support de cours en génie logiciel 2, Cours dispensé à l'Institut Supérieur de Commerce en Deuxième Licence CSI, 2019.
4. - Olivier Guibert, Cours d'analyse et conception des Systèmes d'Informations (Outils et Modèles pour le Génie Logiciel), Département Informatique de l'IUT de l'Université Bordeaux 1. Novembre, 2007.
5. - Delphine Longuet, Introduction au génie logiciel et à la modélisation, Cours au Polytech Paris-Sud Formation initiale 3eme Année Spécialité Informatique Année 2017-2018.

Engineering Title: Computer Security.
Semester: 05.
TU Title:
Subject Title: Advanced Programming.
Credits: 4.
Coefficient: 2.

Teaching Objectives: This course could be a self-study document for a Python programming course. It contains a section for beginners, a discussion of several advanced topics of interest to Python programmers.

Recommended Prior Knowledge: Algorithms, and Object-Oriented Programming.

Course Content:

Part 1- Beginning Python
- Lexical matters.
- Statements and inspection -- preliminaries.
- Built-in data-types.
- Functions and Classes -- A Preview.
- Statements.
- Functions, Modules, Packages, and Debugging.
- Classes.
- Special Tasks.

1.10 More Python Features and Exercises.

Part 2- Advanced Python.
- Regular Expressions.
- Iterator Objects.
- Unit Tests.
- Extending and embedding Python.
- Parsing.
- GUI Applications.
- Guidance on Packages and Modules.
- End Matter.

Part 3- Python Workbook.
- Lexical Structures.
- Execution Model.
- Built-in Data Types.
- Statements.
- Functions.
- Object-oriented programming and classes.
- Additional and Advanced Topics.
- Applications and Recipes.

Part 4- Generating Python Bindings for XML.
- Generating the code.
- Using the generated code to parse and export an XML document.
- Some command line options you might want to know.
- The graphical front-end.
- Adding application specific behavior.
- Special situations and uses.
- Some hints.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. https://www.davekuhlman.org/python_book_01.pdf.
2. Black Hat Python: Python Programming for Hackers and Pentesters, Justin Seitz.
3. The Practice of Network Security Monitoring: Understanding Incident Detection and Response, Richard Bejtlich.

Engineering Title: Computer Security.
Semester: 05.
TU Title:
Subject Title: Web Development.
Credits: 3.
Coefficient: 2.

Teaching Objectives: Mastery of programming and development of applications and Websites.

Recommended Prior Knowledge: Algorithmics, and HMI.

Course Content:
1- Introduction to the Web.
2- Web architecture.
3- Web sites.
4- Web applications.
5- Web design and development.
- HTML5.
- CSS3.
- PHP5.
- SQL
- JAVASCRIPT language.
- jQuery library.
- Other tools.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Francis Draillard, Premiers pas en CSS3 et HTML5, 7e édition mise à jour, Eyrolles, 2017.
2. Patrick Lenormand, Comment dynamiser le contenu de son site web ? Edition PYRAMYD, Collection: Savoir et savoir-faire, 2017.
3. Luc Van Lancker, AJAX - Développez pour le Web 2.0, Entrez dans le code : JavaScript, XML, DOM, XML http Request 2 ... Eni editions, collection : Ressources informatiques. 2015.
4. Jean-Marie Defrance, jQuery-Ajax avec PHP : 44 ateliers pour maîtriser jQuery. Editeur : Eyrolles, 4° édition, Collection : Blanche, 2013.
5. Bogdan Brinzarea, CristianDarie, Audra Hendrix, AJAX et PHP : Comment construire des applications web réactives, Dunod, 2° édition, Collection : InfoPro - Etudes, développement et intégration, 2010.

Engineering Title: Computer Security.
Semester: 05.
TU Title:
Subject Title: Theory of Information and Coding.
Credits: 2.
Coefficient: 1.

Teaching Objectives: The aims of this course are to introduce the principles and applications of information theory. The course will study how information is measured in terms of probability and entropy, and the relationships among conditional and joint entropies; how these are used to calculate the capacity of a communication channel, with and without noise; coding schemes, including error correcting codes; how discrete channels and measures of information generalize to their continuous forms; the Fourier perspective; and extensions to wavelets, complexity, compression, and efficient coding of audio-visual information.

Recommended Prior Knowledge: Basics notions on coding information.

Course Content:
1. Entropy and information, conditional entropy, mutual information.
2. Source coding: Huffman coding, Lempel-Ziv compression.
3. Channel coding.
4. Error Correcting codes, linear codes.
5. Code terminals and wire-tap channels.
6. The main families of block codes.
7. Decoding.
8. Cryptography and cryptanalysis.

Evaluation Mode: Continuous Evaluation, and Exam.

References:

1. William Cary Huffman, and Vera Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2010.
2. David JC MacKay. Information Theory, Inference, and Learning Algorithms, 2003.
3. Olivier Rioul, Théorie de l'information et du codage, 2007.

Engineering Title: Computer Security.
Semester: 05.
TU Title:
Subject Title: Business Intelligence.
Credits: 1.
Coefficient: 1.

Recommended Prior Knowledge: Business notions.

Course Content: Business Intelligence (BI) is a crucial aspect of modern business strategy, focusing on the utilization of data-driven insights to make informed decisions and gain a competitive advantage. This course introduces students to the concepts, technologies, and practices of BI, covering topics such as data warehousing, data mining, analytics, visualization, and decision support systems. Through lectures, case studies, and hands-on projects, students will learn how to collect, analyze, and interpret data to support organizational decision-making and improve business performance.

Course Content:
- Introduction to Business Intelligence.
- Data Warehousing and ETL Processes.
- Data Modeling and Dimensional Design.
- Data Mining and Predictive Analytics.
- BI Tools and Technologies.
- Advanced Analytics and Big Data.
- Business Intelligence Applications and Case Studies.

Evaluation Mode: Exam.

References:

1. MÜLLER, Roland M. et LENZ, Hans-Joachim. Business intelligence. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.
2. HOWSON, Cindi. Successful business intelligence. Emeryville: McGraw-Hill Professional Publishing, 2007.
3. MICHALEWICZ, Zbigniew, SCHMIDT, Martin, MICHALEWICZ, Matthew, et al. Adaptive business intelligence. Springer Berlin Heidelberg, 2006.

Engineering Title: Computer Security.
Semester: 06.
TU Title:
Subject Title: Advanced Cryptography.
Credits: 6.
Coefficient: 4.

Teaching Objectives: Introduce the student to the study of cryptosystems based on algebraic problems or error-correcting code problems.

Recommended Prior Knowledge: Some algebra concepts.

Course Content:

1. Introduction.
   a- Security needs.
   b- Symmetric Crypto-Systems, Asymmetric Crypto-Systems.
   c- Hash Functions.
   d- Electronic Signature.
   e- New Trends in Cryptography.
   f- Cryptanalysis.
2. Encryption, security.
   a- “One-way” function.
   b- The RSA method and factorization of integers.
   c- Discrete logarithm and El Gamel cryptosystem.
   d- The Knapsack problem.
   e- Error correcting codes and Mc Elièce cryptosystem.
   f- Elliptic curves, cryptosystems.
   g- Secret Sharing.
   h- Image encryption.
   i- Copyright protection.
3. Authentication.
   a- Protocols, Principles.
   b- Authentication techniques, digital signature.
   c- Signature using public keys.
   d- File security.
   e- Algorithms, examples.

Evaluation Mode: Continuous Evaluation, and Exam.

References:

1. Ireland & Rosen, A Classical Introduction to Modern Number Theory, Springer.
2. Koblitz, A Course in Number Theory and Cryptography, Springer, 1994.
3. Blake, Seroussi et Smart, Elliptic Curves in Cryptography, Springer.
4. Koblitz, Algebraic Aspects of Cryptography, Springer.

Engineering Title: Computer Security.
Semester: 06.
TU Title:
Subject Title: Modeling & Simulation.
Credits: 6.
Coefficient: 3.

Teaching Objectives: This course is intended to deepen the knowledge of the student in modeling and simulation field. In addition, it introduces techniques of performance evaluation.

Recommended Prior Knowledge: Engineering science, Mathematics, Automation.

Course Content:

I. Systems modeling.
I.1 Definitions.
- I.1.1 Definition of modeling.
- I.1.2 System definition.
- I.1.3 Model definition.

I.2 Types of systems: discrete, continuous, deterministic.
I.3 Types of models: descriptive, analytical.
I.4 Modeling tools.
- I.4.1 Transfer function.
  - I.4.1.1 Definition.
  - I.4.1.2 Laplace transform.
  - I.4.1.3 Block diagrams.
- I.4.2 Finite state machines.
- I.4.3 Petri net.
- I.4.4 Markov chains.
- I.4.5 Queue models.

II. Performance evaluation techniques.
- II.1 Presentation of techniques.
- II.2 Mathematical methods.
- II.3 Introduction to simulation.

III. Simulation.
- III.1 Types of simulation.
  - III.1.1 Simulation of dynamic systems.
  - III.1.2 Continuous simulation.
  - III.1.3 Simulation of discrete systems.
- III.2 Sampling.
- III.3 Generation of pseudo-random numbers.
- III.4 Random number generator tests.
- III.5 Analysis and validation of simulation results.

IV. Simulation tools.
- IV.1 Software.
- IV.2 Languages.
- IV.3 Graphics and simulation.

V. Study of a simulation language.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Youssef Monsef, Modélisation et simulation des systèmes complexes : Concepts, méthodes et outils, Tec & Doc Lavoisier, 1996.
2. Frédéric Amblard, Denis Phan, Modélisation et simulation multi-agents Hermès, Science Publications, 2006.
3. J. Christian Attiogbé, Modélisation et construction des applications réparties, Modélisation avec les Réseaux de Petri, DUT Informatique - Module M-4102C, Janvier 2020.
4. Christophe Sabot, Partie III: chaînes de Markov: Notes informelles de cours, Université Lyon-1, 2020.
5. Yliès Falcone, Jean-Claude Fernandez, Automates à états finis et langages réguliers, Livre, Dunod, 2020.
6. Sara Rachidi, Diagnostic des défauts dans les systèmes à évènements discrets soumis à des contraintes temporelles, Thèse, Normandie Université, 2019.
7. S. Le Digabel, Introduction aux files d'attente, Support de cours, Ecole Polytechnique de Montréal, 2017.

Engineering Title: Computer Security.
Semester: 06.
TU Title:
Subject Title: Cloud Computing.
Credits: 4.
Coefficient: 2.

Teaching Objectives: To allow the student to become familiar with the Cloud Computing, by presenting the foundations of virtualization as well as the tools to create and deploy Cloud infrastructures.

Recommended Prior Knowledge: Notions of virtualization, distributiveness, network, Web, ...

Course Content:

Chapter I. Definitions and History.
- I.1. Definitions.
  - I.1.1. The Cloud, and the Cloud Computing.
  - I.1.2. Cloud Computing from an Economic View Point.
  - I.1.3. The Cloud Computing: A Virtual Space.
- I.2. Historic.
  - I.2.1. The 50's.
  - I.2.2. Early 2000s.

Chapter II. Cloud Computing Models and Services.
- II.1. Cloud Model.
- II.2. Cloud Services.
  - II.2.1. Infrastructure as a Service: IaaS.
  - II.2.2. Platform as a Service: PaaS.
  - II.2.3. Software as a Service: SaaS.
  - II.2.4. Cloud Services Architecture.
  - II.2.5. Other Services.

Chapter III. Architecture and Typology of Cloud Computing.
- III.1. Architecture.
  - III.1.1. N-Tiers.
  - III.1.2. Service Oriented Architecture (SOA).
  - III.1.3. Virtual Machine.
  - III.1.4. File Virtualization.
- III.2. Deployment.
  - III.2.1. Pilot Phase.
  - III.2.2. Deployment and Integration Phase.
  - III.2.3. Loading Driving Phase.
- III.3. Typology.
  - III.3.1. Private Cloud.
  - III.3.2. Public Cloud.
  - III.3.3. Community Cloud.
  - III.3.4. Hybrid Cloud.
  - III.3.5. Distributed Cloud.
  - III.3.6. Inter Cloud.
  - III.3.7. Multi Cloud.

Chapter IV. Cloud Examples.

IV.1. DROPBOX.
IV.2. Microsoft Cloud Platform.
IV.3. Commercials Clouds, and Main Market Players.
IV.5. OpenStack Overview.
IV.6. Examples of Cloud for Storage.

Chapter V. Benefits and Limits of the Cloud.

V.1. Benefits of the Cloud.
V.1.1. Cost Reduction.
V.1.2. Flexibility.
V.1.3. Refocusing on the Core Business.
V.2. Cloud Limitation.
V.2.1. Control Loss of Your IT (Entrusted to One or Third Parties).
V.2.2. Problems with Securing its Computer Data.

Chapter VI. Security and Privacy in the Cloud.

VI.1. General Aspects.
VI.2. Specific Security Issues.
VI.3. Contractual Aspects.
IV.4. Best Security Practices.
IV.5. Synthesis and Overview.
IV.5.1. Threat.
IV.5.2. Attackers Types.
IV.5.3. Security Risks.
IV.5.4. Advice for Limiting Risks.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, "Cloud Computing : Principles and Paradigms", John Wiley & Sons, 2010 (ISBN 9781118002209).
2. Lee Gillam, "Cloud computing", Springer, 2010 (ISBN 9781849962414).
3. Zaigham Mahmood, Richard Hill, "Cloud Computing for Enterprise Architectures", Springer, 2011 (ISBN 9781447122364).
4. Cigref Réseau des grandes entreprises, "Fondamentaux du Cloud Computing – Le point de vue des grandes entreprises", Mars 2013.
5. Romain Hennion, Hubert Tournier, Eric Bourgeois, Cloud Computing : Décider - Concevoir - Piloter - Améliorer, Eyrolles, 2012.
6. Guillaume Plouin, Cloud Computing, Sécurité, stratégie d'entreprise et panorama du marché, Collection InfoPro, Dunod, 2013.
7. Guillaume Plouin, Tout sur le Cloud Personnel, Travaillez, stockez, jouez et échangez... dans le nuage, Dunod, 2013.

Engineering Title: Computer Security.
Semester: 06.
TU Title:
Subject Title: Advanced Databases.
Credits: 4.
Coefficient: 2.

Teaching Objectives: Follows the evolution of the IT context and the advent of system applications in existing databases while showing current trends. The course will also deal with database security.

Recommended Prior Knowledge: Concepts on Database, DBMS

Course Content:

1. Extended relational model
2. Semantic models (SDM, AI, etc.)
3. Object-oriented databases
4. Deductive databases
5. Distributed databases
6. Multimedia databases
7. Secure Databases and database security

Evaluation Mode: Continuous evaluation, and exam.

References:

1. G. Gardarin & P.Valduriez: “Advanced DBMS” Editions Eyrolles, 1990.
2. J. Le Maitre “Advanced databases for XML and the web” Hermes Science Publications, 2005.
3. J.Date. Introduction to databases. Thomason publishing France 6th edition 1998.
4. C. Delobel and M. Adiba: databases and relational systems. Dunod 1982.
5. T. Connoly and Corolyn Begg. Database systems: practical approach to design of implementation and administration. Eyrolles 2005.
6. Lena Wiese, Advanced data management: for SQL, NoSQL, Cloud and distributed databases, De Gruyter, 2015.
7. Christopher Diaz, Database Security: Problems and Solutions, Mercury Learning and Information, 2022.

Engineering Title: Computer Security.
Semester: 06.
TU Title:
Subject Title: Mobile Development.
Credits: 3.
Coefficient: 2.

Teaching Objectives: The student will acquire knowledge of application development in mobile environments. They are omnipresent whether you are a customer (BtoC), supplier (BtoB) or employee (BtoE). He will learn programming under Android, its development platform and the specificities of embedded development on smartphones.

Recommended Prior Knowledge: Web development.

Course Content:

Chapter 1: Mobile applications.
- Mobile Operating Systems.
- Mobile Applications Types.

Chapter 2: Android Platform.
- Presentation of the Android platform.
- The fundamental components of an Android application.
- Android SDK.
- Installation and configuration of tools.
- Create an Android Emulator.

Chapter 3: Activities and resources.
- Concept of Activity.
- Life cycle of an activity.
- Resources, Organization of resources, and utilization.

Chapter 4: GUIs and Widgets.
- Creation of graphical interfaces.
- Manage events on widgets.

Chapter 4: Menus and dialog boxes.
- Management of application menus, Options menu, and Context menus.
- Dialog boxes.

Chapter 4: Communication between components: Explicit intents, Implicit intents, and Resolving Implicit Intents.
Chapter 5: Databases with SQLite.
Chapter 6: Development of an application.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Create apps for Android – Open Classrooms https://openclassrooms.com/courses/creez-es-applications-pour-android.
2. Android Development - Jean-Francois Lalande, http://www.univ-orleans.fr/lifo/Members/Jean-Francois.Lalande/enseignement/android/cours-android.pdf.

Engineering Title: Computer Security.
Semester: 05.
TU Title:
Subject Title: Digital Signal Processing.
Credits: 4.
Coefficient: 2.

Teaching Objectives: This course introduces the basic concepts and principles underlying Continuous and discrete-time signal processing. The objective is to analyze, manipulate, and interpret signals to extract useful information or enhance their quality for various applications. The Concepts will be illustrated using examples of standard technologies and algorithms.

Recommended Prior Knowledge: Signal theory, applied mathematics.

Course Content:

Chapter I. Introduction to Signal Processing.

1. Signal and System.
2. Signal Classification.
3. Frequency and Time Representation.

Chapter II. Analog Signal Processing.

1. Fourier Series.
2. Fourier Transform.
3. Convolution.
4. Filtering Concept.
5. Modulation Concept.

Chapter III. Digital Signal Processing.

1. Sampling.
2. Quantization.
3. Coding.
4. The Discrete Fourier Transform (DFT).
5. Discrete Fourier Transform: Derivation of Radix-2 FFT.

Chapter IV. Fast Algorithms for Signal Processing.

1. Fast Convolution Algorithm.
2. Fast Fourier Transform Algorithm.
3. Multidimensional Transform Algorithms.
4. Algorithms Derived from the Fourier Transform.

Chapter V. Wavelet Transform and Time-Frequency Analysis.

1. Multiresolution Analysis, Splines, and Wavelets.
2. Orthogonal Decomposition of Wavelet Series.
3. Wavelet Decompositions and Reconstructions.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Francis Cottet, Traitement des signaux et acquisition de données, Dunod, 1997.
2. J. Sundberg, Le chant, Les instruments de l'orchestre" (Préfacé par J. C. Risset), Bibliothèque pour la science, 1995.
3. Neville H. Fletcher, Thomas D. Rossing, The Physics of musical Intruments, SpringerVerlag, 1991.
4. Donald E. Hall, Musical Acoustics, An introduction, Wadsworth, California, USA, 1980.

Engineering Title: Computer Security.
Semester: 06.
TU Title:
Subject Title: AI: Notions & Principles.
Credits: 2.
Coefficient: 1.

Teaching Objectives: Acquisition of fundamental and preliminary notions about AI.

Recommended Prior Knowledge: Difference between natural and artificial intelligence.

Course Content:

Chapter 1: Birth of AI.

1- History: birth of AI, type of problem that AI addresses, and difference compared to computational computing.
2- Turing test.
3- Field of application of AI.

Chapter 2: Expert system.

1- Role definition.
2- Architecture of an OS.

Chapter 3: Operation of expert systems.

1- Notion of knowledge and representation formalism.
2- Production rules.
3- Operation of an inference engine.

Chapter 4: Approach to developing an expert system.

1. Expert system development process.
2. Example of an expert system: Dendral, Mycin, Prospector, etc.

Evaluation Mode: Exam.

References:

1. Louis Frécon, and Okba Kazar, Artificial intelligence manual, PPUR edition, ISBN:978-2-88074-819-7, 2009.
2. Ganascia, Jean-Gabriel, Artificial intelligence, Flammarion, 1993.
3. I. Bratko, Prolog programming for artificial intelligence, 2001.
4. J.M. Alliot, and T. Schiex, Artificial Intelligence, and Theoretical Computing, Cépaduès Editions, 1993.
5. N. Nilsson, Artificial Intelligence: A New Synthesis, Morgan Kaufmann, 1998.
6. S. Russell, and P. Norvig, Artificial Intelligence: A Modern Approach, 2nd edition, 2002.

Engineering Title: Computer Security.
Semester: 06.
TU Title:
Subject Title: Startup and Professional Development.
Credits: 1.
Coefficient: 1.

Teaching Objectives:
- Understand the principles of entrepreneurship and startup development.
- Develop skills in idea generation, validation, and business model canvas creation.
- Learn effective pitching techniques and strategies for attracting investors.
- Gain insights into startup funding options and the venture capital landscape.
- Master professional development skills tailored for computer science students, including resume writing, networking, and job searching.
- Prepare for technical interviews and learn best practices for securing internships and full time positions in the tech industry.
- Explore avenues for career advancement and personal growth within the tech sector.

Recommended Prior Knowledge: Advanced business concepts.

Course Content:
1. Introduction to Startups.
2. Idea Generation and Validation.
3. Business Model Canvas.
4. Pitching and presenting.
5. Startup Funding.
6. Professional Development for Computer Science Students.
7. Job Searching Strategies.
8. Interview Preparation.
9. Internships and Co-op Programs.
10. Career Advancement in Tech.

Evaluation Mode: Exam.

References:
1. Ries, Eric. The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses. New York: Crown Business, 2011.
2. Thiel, Peter, Zero to One: Notes on Startups, or How to Build the Future. Books on Tape, 2014.

Engineering Title: Computer Security.
Semester: 07.
TU Title:
Subject Title: Advanced Operating Systems.
Credits: 5.
Coefficient: 3.

Teaching Objectives: The objective of this course is to provide an in-depth study of the problems encountered in systems centralized and distributed operating systems. The basic mechanisms proposed for the resolution of the parallelism, mutual exclusion, synchronization, inter-process communication and deadlock are studied in detail. Directed and practical work allows students to manipulate and master the use of the basic mechanisms of the operating systems studied theoretically.

Recommended Prior Knowledge: basic notions of operating systems, algorithms, machine structure, and the mechanisms allowing the management of machine resources, in particular the processor and memory.

Course Content:
Chapter 1: Notions of parallelism, cooperation and competition.
- a. Sequential processes.
- b. Concept of task.
- c. Task systems and precedence graph.
- d. Task system language.
- e. Task system state.
- f. Determinism and maximal parallelism.
- g. Cooperation and competition.
- h. Thread concept.

Chapter 2: Synchronization between processes.
- a. Mutual exclusion problem.
- b. Implementation of mutual exclusion (lock, alternation, Peterson, TSL, sleep primitives, and wakeup).
- c. Synchronization problem.
- d. Implementing synchronization (event counters, semaphores, monitors).

Chapter 3: Inter-process communication.
- a. Problematic.
- b. Exchange of messages.
- c. Mail boxes.
- d. Communication tubes under Unix.
- e. Signals.
- f. Sharing variables (variables, files, data segments).
- 4. Chapter 4: Deadlock.
- a. Introduction.
- b. Deadlock.
- c. Necessary conditions for deadlock.
- d. Solutions to the deadlock problem.
- e. Detection and recovery.
- f. Deadlocks avoidance.
- g. Prevention of deadlocks: PERSONAL WORK.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. J-L. Peterson, F. Silbershartz , P-B. Galvin ‘Operating Systems Concepts’, Fourth Edition.
2. A. Silberschatz, P-B. Galvin, ‘Principes des systèmes d’exploitation’, 4ème Edition, AddisonWesley.
3. J. Beauquier, B. Berard ‘Systèmes d’exploitation : concepts et algorithmes’, McGraw Hill 1990.
4. M-J. Bach, traduit par G. Feallah, ‘Conception du Système UNIX’, Masson et Prentice Hall 1990.
5. A. Tanenbaum, ‘Modern operating systems’, third edition, Pearson, 2014.
6. A. Tanenbaum, ‘Système d’exploitation’, Dunod, 1994.
7. M. Divay, ‘Unix, Linux et les systèmes d'exploitation : cours et exercices corrigés’, 2004.
8. Crocus, ‘Systèmes d'exploitation des ordinateurs’, 1993.
9. S. Krakowiak, ‘Principes des systèmes d'exploitation des ordinateurs’, Dunod, 1993.

Engineering Title: Computer Security.
Semester: 07.
TU Title:
Subject Title: Advanced Networks.
Credits: 5.
Coefficient: 3.

Teaching Objectives: This module aims to provide students with an in-depth understanding of advanced concepts, protocols, and technologies in computer networks. It builds upon foundational knowledge in networking and explores topics such as network security, emerging technologies, and advanced network architectures. Through lectures, practical exercises, and case studies, students will develop the skills and expertise necessary to design, implement, and manage complex computer networks.

Recommended Prior Knowledge: Students should have a solid understanding of basic networking concepts, protocols, and technologies, as well as proficiency in network configuration and troubleshooting. Prior knowledge of programming languages, particularly Python or similar scripting languages, may be beneficial for certain topics such as network automation and SDN.

Course Content:

1. Introduction to Advanced Computer Networks.
   - o Overview of the module objectives, structure, and assessment criteria.
   - o Review of fundamental networking concepts and protocols.
   - o Introduction to advanced networking topics and their relevance in modern network environments.
2. Network Security.
   - o Threats, vulnerabilities, and attacks in computer networks.
   - o Cryptography and encryption techniques for securing data transmission.
   - o Firewalls, intrusion detection systems, and other security mechanisms.
   - o Secure network design principles and best practices.
3. Quality of Service (QoS).
   - o Overview of QoS requirements and challenges in modern networks.
   - o Traffic shaping, prioritization, and scheduling techniques.
   - o QoS mechanisms in different network architectures, such as DiffServ and MPLS.
   - o Case studies and practical exercises on QoS implementation.
4. Emerging Network Technologies.
   - o Introduction to emerging technologies such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Internet of Things (IoT).
   - o Overview of their architecture, protocols, and applications.
   - o Case studies and practical demonstrations of emerging network technologies.
5. Advanced Routing and Switching.
   - o Routing protocols beyond basic routing algorithms (e.g., OSPF, BGP).
   - o Advanced switching techniques and protocols (e.g., VLANs, Spanning Tree Protocol).
   - o Scalability, resilience, and performance considerations in routing and switching.
6. Network Management and Monitoring.
   - o Network management frameworks and protocols (e.g., SNMP, NetFlow).
   - o Configuration management, fault detection, and performance monitoring.
   - o Network troubleshooting methodologies and tools.

7. Wireless and Mobile Networks.
   o Overview of wireless communication principles and technologies.
   o Mobile network architectures (e.g., 4G/5G) and protocols (e.g., GSM, LTE).
   o Security, QoS, and mobility management in wireless and mobile networks.
8. Case Studies and Practical Applications.
   o Real-world case studies of advanced network deployments and implementations.
   o Hands-on lab sessions and practical exercises to reinforce theoretical concepts.
   o Project work or assignments focusing on designing and implementing advanced network solutions.
9. Future Trends and Challenges.
   o Exploration of future trends and developments in computer networks.
   o Discussion of emerging technologies, challenges, and opportunities.
   o Ethical, legal, and societal implications of advanced network technologies.

Evaluation Mode: Continuous evaluation, and exam.

References:

- Textbooks:
1. "Computer Networking: A Top-Down Approach" by James F. Kurose and Keith W. Ross.
2. "Computer Networks" by Andrew S. Tanenbaum and David J. Wetherall.
3. "TCP/IP Illustrated" by Richard Stevens.
- Online Resources:
1. Cisco Networking Academy: https://www.netacad.com/.
2. Coursera: Various courses on computer networking and cybersecurity.
3. IEEE Xplore and ACM Digital Library for research papers and articles on advanced networking topics.
- Software Tools:
1. Packet Tracer or GNS3 for network simulation and emulation.
2. Wireshark for network protocol analysis.
3. Open-source software for SDN experimentation (e.g., Mininet, OpenDaylight).

Engineering Title: Computer Security.
Semester: 07.
TU Title:
Subject Title: Computer Systems Security.
Credits: 5.
Coefficient: 2.

Teaching Objectives: One of the main objectives of this course is adversarial thinking: students should be able to quickly zoom in on the weakest link in any security technology, or system design. Students should be able to imagine how an attacker might break their system, and build in protection and mitigation measures to ward off such attacks.

Recommended Prior Knowledge: Concept of computer security.

Course Content:
- Principles and practice of building and administering secure systems.
- Authentication and access control.
- Operating system security.
- Program security.
- Key management.
- Information flow.
- Assurance.
- Vulnerability analysis and intrusion detection.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Stamp, Mark, Information Security: Principles and Practice (2nd Edition), Wiley, 2011, ISBN: 978-0-470-62639-9.
2. Anderson, Ross, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, Wiley Publishing, Inc., 2008, ISBN: 978-470-06852-6 [https://www.cl.cam.ac.uk/~rja14/book.html].

Engineering Title: Computer Security.
Semester: 07.
TU Title:
Subject Title: Information and Data Security.
Credit: 5.
Coefficient: 2.

Teaching Objectives: This course allows students to acquire skills to ensure the security and proper functioning of computer systems.

Recommended Prior Knowledge: Algorithmic foundation, programming technique.

Course Content:

I.1. Definitions: Security, Dependability, etc.
I.2. Main information security concepts: Vulnerability, threat, countermeasure, risk, ...
I.3. Information security objectives: Confidentiality, Integrity, Availability, Non-repudiation, Authentication.
I.4. Security types.
I.5. Security flaws.
I.6. Risk management process.
I.7. Risks typology and proposed solutions.
I.8. IT threats.
- What is an attack?
- Attacks motivations.
- Origin of attacks.
- Who can be targeted?
- Stages of an attack.
- Different taxonomies of attacks.
- Different types of attacks: Network attacks, System attacks, Password attacks, Website attack, application attack.
- Ways to launch an attack.
- Flaws and attacks (IP Spoofing, DoS, phishing, …).
- Malware: Virus, Worm, Trojan horse, Spyware, …

I.9. Defense methods: Anti-virus, Firewalls, Private networks, Intrusion detection, etc...

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Laurent Bloch, Christophe Wolfhugel, AryKokos, Gérôme Billois, Arnaud Soullié, Alexandre AnzalaYamajako, Thomas Debize, Sécurité informatique pour les DSI, RSSI et administrateurs, éditions Eyrolles, 5° édition, Collection Blanche, 2016.
2. Jean-François Pillou, Jean-Philippe Bay, Tout sur la sécurité informatique, DUNOD, 4° EDITION, 2016.
3. Gilles Dubertret, L'univers secret de la cryptographie, Vuibert, 2015.
4. Damien Vergnaud, Exercices et problèmes de cryptographie, Collection : Sciences Sup, Dunod, 2015.

Engineering Title: Computer Security.
Semester: 07.
TU Title:
Subject Title: Programming by Constraints.
Credit: 3.
Coefficient: 2.

Teaching Objectives: Allow the student to use constraint programming techniques for solving complex combinatorial problems from logic programming and artificial intelligence.

Recommended Prior Knowledge: Problem solving in artificial intelligence using logic programming, Combinatorial Optimization.

Course Content:

1- General information on Constraint Programming (CP).
- Introduction to Constraint Programming.
- Definition and fundamental principles of CP.
- Applications of CP in various fields.
- Examples of problems solved by CP.

2- Constraint Modeling.
- Representation of variables and constraints.
- Types of constraints and their properties.
- Global constraints and local constraints.
- Modeling techniques for specific problems.
- Modeling in Constraint Satisfaction Problem (CSP).
- Card Colorability, Magic Square, Golomb Rule, the n Queens, Euler's knight.
- Binarization.
  Binary CSP, Boolean CSP, Binary CSPs, n-ary CSPs.

3- Resolution Methods in CP.
- Systematic research techniques (backtracking, branch and bound).
- Constraint propagation and filtering algorithms.
- Heuristic search strategies (variable ordering, value ordering).

4- Practical Applications of PPC.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Thom Frühwirth et Slim Abdennadher, Essentials of Constraint Programming, Springer, Avril 2003, 145 p.
2. Francesca Rossi, Peter Van Beek et Toby Walsh, Handbook of constraint programming, Elsevier, 2006.
3. Annick Fron, Programmation par Contraintes, The Book Edition.
4. Trends in Constraint Programming, edited by Frédéric Benhamou, Narendra Jussien, Barry O'Sullivan, © ISTE Ltd, 2007.

Engineering Title: Computer Security.
Semester: 07.
TU Title:
Subject Title: Machine Learning, Deep Learning, and Security.
Credit: 4.
Coefficient: 2.

Teaching Objectives: Understand ML and DL techniques and apply them to resolve security issues.

Recommended Prior Knowledge: IA Notions.

Course Content:

1. Machine Learning (ML).
   - o Concepts.
   - o Challenges of using Machine Learning.
   - o Necessary tools for practicing Machine Learning on your own data.
   - o Setting up a workflow.
   - o Python (NumPy, Pandas, Matplotlib, Seaborn...).
   - o Importance of data visualization.
   - o Explore, manage and prepare data.
   - o Choose and apply a good algorithm.
   - o Understand the difference between a supervised context and an unsupervised context.
   - o Supervised algorithms.
   - o Unsupervised algorithms.
   - o Deploy the Machine Learning model.
   - o Conditions for deploying a Machine Learning model.
2. Deep Learning (DL).
   - o Introduction to artificial neural networks.
   - o Train a PMC (Multi-Layer Perceptron) with a high-level TensorFlow API.
   - o Train a PMC (MultiLayer Perceptron) with basic TensorFlow.
   - o Precisely adjust the hyperparameters of a neural network.
   - o Training of deep neural networks.
   - o Convolutional neural networks.
   - o Recurrent neural networks.
3. Traditional Machine Learning and cybersecurity.
   - o Spam Detection.
   - o Intrusion Detection.
   - o Malware Detection.
3. Case study: Solving network and security problems with DL-ML solutions.
   - o Routing issues.
   - o Problems with access and migration to resources.
   - o Scalability issues.
   - o Threat and vulnerability detection issues.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. John Paul Mueller, « Machine Learning Security Principles: Keep data, networks, users, and applications safe from prying eyes », 2022.
2. Aaisha Makkar, Neeraj Kumar « Deep Learning for Security and Privacy Preservation in IoT (Signals and Communication Technology) », Springer, 2022.

Engineering Title: Computer Security.
Semester: 07.
TU Title:
Subject Title: Malwares Analysis.
Credit: 2.
Coefficient: 2.

Teaching Objectives: This course aims to provide students with an in-depth understanding of malware and its attack techniques and acquire advanced skills in malware analysis by combining static, dynamic and behavioral approaches with the hybrid method and reverse engineering. It also prepares students to identify, analyze and neutralize complex and emerging malware.

Recommended Prior Knowledge: Concepts on IT security risks and vulnerabilities.

Course Content:

Chapter 1: Fundamentals of Malware Analysis.
- Fundamental concepts of Malware.
- Types of Malwares and their behaviors.
- Analysis of the evolution of attack techniques and defenses against Malware.

Chapter 2: Static Analysis.
- Static Malware analysis techniques.
- Disassembly, decompilation and code analysis.
- Identification and extraction of malicious features and behaviors.

Chapter 3: Dynamic Analysis.
- Dynamic Malware analysis techniques.
- Sandboxing and volatility analysis.
- Real-time monitoring of Malware interactions with the system and network.

Chapter 4: Behavioral Analysis.
- Observation and understanding of the actions of the Malware on the infected system.
- Analysis of Indicators of Compromise (IoC) and malicious behavioral patterns.

Chapter 5: Hybrid Analysis Methodology.
- Principles of the hybrid method.
- Integration of static, dynamic and behavioral approaches for a complete analysis.

Chapter 6: Reverse engineering techniques.
- Introduction to reverse engineering and its applications in Malware analysis.
- Use of reverse engineering tools (IDA Pro, Ghidra, and Radare2) to analyze malicious code.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. "Practical Malware Analysis: The Hands-On Guide to DissectingMalicious Software" par Michael Sikorski et Andrew Honig.
2. "The IDA Pro Book: The Unofficial Guide to the World's Most PopularDisassembler" par Chris Eagle.
3. Articles et publications académiques sur les dernières avancées en matière d'analyse de malwares et de reverse engineering.

Engineering Title: Computer Security.
Semester: 07.
TU Title:
Subject Title: Critical Thinking and Creativity Skills.
Credit: 1.
Coefficient: 1.

Teaching Objectives:
The aim of this course is to introduce the concept of critical thinking and its importance as well as give students the tools necessary to develop their critical thinking abilities and creativity skills.

Recommended Prior Knowledge: None.

Course Content:
1. Introduction: Importance of skills for future employment. Importance of creativity and critical thinking as soft skills.
2. Introduction to analytical thinking, identifying, and evaluating arguments.
3. Various problem-solving methodologies.
4. Decision-making processes and risk analysis
5. Understanding logical fallacies and avoiding them in decision-making.
6. Exploring creativity, fostering a creative mindset, mind mapping and brainstorming, convergent and divergent thinking.
7. Critical Thinking in Coding: debugging and code review.
8. Integrating critical thinking and creativity for effective problem-solving.
9. Final Project and Presentation: students will integrate what they learned in a final project.

Evaluation Mode: Exam (Final project presentation).

References:

1. Proctor, T. (2021). Absolute Essentials of Creative Thinking and Problem Solving. Rutledge, London.
2. Jamie Carlin Watson, Robert Arp, Skyler King, Critical Thinking: An Introduction to Reasoning Well, Bloomsbury Academic, 2024.
3. Joseph O'Connor, Ian McDermott, The Art of Systems Thinking: Essential Skills for Creativity and Problem Solving, Thorson, 1997.
4. Stella Cottrell, Critical Thinking Skills: Effective Analysis, Argument and Reflection, Bloomsbury Study Skills, 2023.
5. Michael Lewrick , Patrick Link, Larry Leifer, The Design Thinking Toolbox: A Guide to Mastering the Most Popular and Valuable Innovation Methods, Amazon, 2020.
6. David Cotton, The Smart Solution Book: 68 Tools for Brainstorming, Problem Solving and Decision Making, FT Publishing International, 2016.

Engineering Title: Computer Security.
Semester: 08.
TU Title:
Subject Title: Operating System Security.
Credit: 5.
Coefficient: 2.

Teaching Objectives: The objective of this course is to allow the student to master the security of operating systems: the basic concepts, methods of analysis and evaluation of the security of operating systems (desktop and mobile). The student will learn about issues related to authentication, access control, and control flow integrity.

Recommended Prior Knowledge: Full Operating systems and the basics of computer security.

Course Content:

1 - Introduction to operating system security (Linux, Windows, and Android).
2- Introduction to operating system administration and access control (Linux, Windows, and Android).
3 - Attacks on Oss.
4 - Operating system protection mechanisms.
5 - Methods for analyzing and evaluating the security of an operating system.
6 - Failure recovery and recovery methods.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Silberschatz. A., Galvin. P., Gagne. G., “Operating System Concepts”, John Wiley & Sons, 2012.
2. Tanenbaum. A.,“Systèmes d’Exploitation”, Pearson, 2008.
3. Jaeger, Trent, Operating system security, Morgan & Claypool Publishers, 2008.
4. Andrew S. Tanenbaum, Herbert Bos, Modern Operating Systems, Pearson, 2023.

Engineering Title: Computer Security.
Semester: 08.
TU Title:
Subject Title: Cybersecurity.
Credit: 5.
Coefficient: 3.

Teaching Objectives: The objectives of this course are to raise awareness about the importance of cybersecurity in today's digital world particularly in the context of businesses, equipping the students with foundational knowledge to protect themselves online, fostering a culture of security and responsibility, preparing them to comply with cybersecurity regulations and standards, and supporting their professional development in cybersecurity-related fields.

Recommended Prior Knowledge: Basic concepts of computer security and digital vulnerability analysis.

Course Content:

Chapter 1: Concepts of Cybersecurity.
- Cybersecurity definition.
- Cybersecurity objectives.
- Importance of cybersecurity in a digital world.
- Cybersecurity approaches.

Chapter 2: Privacy Protection techniques.
- Importance of online privacy protection.
- Principles of privacy Protection.
- Tools and technologies for online privacy protection (e.g. Ad Blockers, Password managers, Privacy-focused Browsers, ...).
- Best practices for secure handling of data.

Chapter 3: DarkWeb and Cybersecurity.
- DeepWeb and DarkWeb.
- Defending against the DarkWeb: Strategies of Protection.
- Tor browsers and the dark web: access and risks.

Chapter 4: Security Detection Tools.
- Firewall/ Web Application Firewall (FW/WAF).
- Proxy.
- Intrusion Detection System/Intrusion Prevention System (IPS/IDS).
- Endpoint Detection and Response (EDR).

Chapter 5: Security Incident Management Tools (SIEM, SOAR, Ticketing tool).
- Logs.
- Security Information and Event Management (SIEM).
- Ticketing systems.
- Security Orchestration Automation and Response (SOAR).

Chapter 6: Security Incident Response.
- Company security teams (SOC/CERT).
- Security rules creation (Use cases).
- Open-source investigation tools.
- Security incident response steps.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Whitman, M. E., & Mattord, H. J. (2016). Principles of Information Security. Cengage Learning.
2. Vacca, J. R. (2014). Computer and Information Security Handbook. Morgan Kaufmann.
3. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
4. Goodrich, M. T., & Tamassia, R. (2014). Introduction to Computer Security. Pearson Education.
5. Rouse, M. (2018). Cybersecurity. Search Security.
6. Emily Darby, and Thomas J. Holt (2017). Cybercrime and the Darknet: Revealing the Hidden Underworld of the Internet, International Journal of Cyber Criminology.
7. Bishop, M. (2003). Computer Security: Art and Science. Addison-Wesley.
8. Bejtlich, R. (2013). The Practice of Network Security Monitoring: Understanding Incident Detection and Response.
9. J.W. Ritti, and J. M. Chiarelli (2017). Cybersecurity Operations Handbook.

Engineering Title: Computer Security.
Semester: 08.
TU Title:
Subject Title: Network Security.
Credit: 5.
Coefficient: 3.

Teaching Objectives: This course aims to provide students with an in-depth understanding of securing networks, regardless of their type or architecture. Primary objectives include the ability to identify best practices, tools and methodologies for analyzing and evaluating network security, as well as the design and implementation of secure network architectures.

Recommended Prior Knowledge: Basic concepts of computer security and digital vulnerability analysis.

Course Content:

Chapter 1: Introduction to Network Security.
- Examples of Network Architectures.
- Common Network Threats and Attacks.
- Surveillance and Prevention.
- Threat Analysis (Tools).
- Network Security Standards.

Chapter 2: Network Security Infrastructures.
- Virtual LAN (VLAN).
- Access Security (Firewall, WAF, Proxy, NAC).
- Server Security.
- Intrusion Prevention and Detection Systems (IDPS).
- Demilitarized Zones (DMZ).
- Virtual Private Networks (VPN).
- Principles and methods for designing a secure network architecture.

Chapter 3: Network Security Policies and Approaches.
- Zero Trust solution.
- SIEM (Security Information and Event Management) solutions.
- IDS/IPS (Intrusion Detection System/Intrusion Prevention System) solutions.
- Access Security.
- Vulnerability Management.
- Audit and Compliance.
- Training and Awareness.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. William Stallings, "Network Security Essentials: Applications and Standards", Pearson, 2016.
2. Razi Rais, Christina Morillo, Evan Gilman, “Zero Trust Networks: Building Secure Systems in Untrusted Networks”, 2nd Edition, Oreilly, 2024.

Engineering Title: Computer Security.
Semester: 08.
TU Title:
Subject Title: Wireless and Mobile Network Security.
Credit: 5.
Coefficient: 3.

Teaching Objectives: This course aims to provide students with an in-depth understanding of securing networks, regardless of their type or architecture. Primary objectives include the ability to identify best practices, tools and methodologies for analyzing and evaluating network security, as well as the design and implementation of secure network architectures.

Recommended Prior Knowledge: Basic concepts of computer security and digital vulnerability analysis.

Course Content:

1. Wireless network security.
   1.1. Encryption of Wifi networks.
   1.2. Threats to Wifi networks.
   1.3. Bluetooth attacks.
   1.4. Wireless Network Vulnerabilities.
   1.5. Securing Wireless Networks.
      - The WEP protocol and its vulnerabilities.
      - The 802.1X protocol and network access control.
      - The 802.11i/WPA Enterprise protocol.
      - Identity and access management (IAM) strategies for wireless networks.
   1.6. Secure configuration of wireless access points (APs).
   1.7. Secure deployment of wireless networks.
   1.8. Implementation of wireless network security policies.
2. Mobile network security.
   2.1. Mobile security threats.
   2.2 Linux Kernel level security.
      - Linux permissions.
      - Linux capabilities.
      - SELinux: Security Enhanced Linux.
      - Other features.
   2.3 Security at Dalvik level.
      - Permissions at Dalvik level.
      - Dalvik code signing.
   2.4 User-level security.
      - The lock screen.
      - Multi-user support.
      - Management of secret and private keys.
      - Certificate management.
   2.5 Storage security.
      - Data encryption.
      - Secure boot.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. William Stallings, 5G Wireless: A Comprehensive Introduction, Addison-Wesley Professional, 2021.
2. Khaldoun Al Agha, Guy Pujolle, Tara Ali-Yahiya,' Mobile and Wireless Networks', Wiley, 2016.
3. Steve Rackley, 'Wireless Networking Technology: From Principles to Successful Implementation', Newnes, 2007.
4. Jennifer (JJ) Minella, Wireless Security Architecture: Designing and Maintaining Secure Wireless for Enterprise, Wiley 2022.
5. Hardeep Singh, Kali Linux Wireless Pentesting and Security for Beginners, 2023.

Engineering Title: Computer Security.
Semester: 08.
TU Title:
Subject Title: Identity & Access Management.
Credit: 2.
Coefficient: 1.

Teaching Objectives: Identity and access management encompasses the tools and processes that are used to verify the identity of users and employees, authorize their access to defined resources (applications, tools, data), and monitor their actions.

Recommended Prior Knowledge: Basic concepts on identification and access rules.

Course Content:

Chapter 1: Introduction to Identity and Access Management (IAM).
- Definitions and fundamental concepts.
- Importance of IAM in IT security.

Chapter 2: IAM Basics.
- Authentication and authorization.
- Identity management: creation, modification, deletion.
- Access management: rights and permissions.

Chapter 3: IAM Models.
- Centralized model vs. decentralized.
- Role-Based Access Control model (RBAC).
- Attribute-Based Access Control model (ABAC).

Chapter 4: IAM Technologies and Tools.
- LDAP directory.
- ID Management systems (IDM).
- Privileged Access Management (PAM) solutions.
- Multi-Factor Authentication solutions (MFA).
- On-premises deployment vs. in the Cloud.
- Integration with existing applications and services.
- Compliance and regulatory considerations.

Chapter 6: Emerging Trends in IAM.
- Adaptive IAM.
- Integration of IAM with AI and Machine Learning.
- Evolution towards a zero-trust approach.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. "NIST Special Publication 800-63: Digital Identity Guidelines" du National Institute of Standards and Technology (NIST) (2020).
2. "IAM Maturity Model: A Framework for Identity and Access Management", Gartner (2018).

Engineering Title: Computer Security.
Semester: 08.
TU Title:
Subject Title: Secure Software Development.
Credit: 4.
Coefficient: 2.

Teaching Objectives: This course aims to provide students with an in-depth understanding of the fundamental principles of software security from the design phase. It also allows learners to acquire skills in integrating security throughout the software development lifecycle (DevSecOps). At the end of this subject, the student is expected to be able to implement management practices effective security in software development, deployment and maintenance.

Recommended Prior Knowledge: Software development approaches and basic notions of IT security.

Course Content:

Chapter 1: Introduction to Software Security.
- Fundamentals of software security.
- Importance of security from the design phase.
- Evolving security practices in software development.

Chapter 2: Security by Design.
- Security principles by design.
- Integration of security into software development processes.
- Threat modeling and risk assessment.

Chapter 3: DevSecOps: Integrating Security into Development and Operations.
- Concepts and principles of DevSecOps.
- Security Automation in DevOps Pipelines.
- Continuous vulnerability and patch management.

Chapter 4: Security Practices in Software Development.
- Static and dynamic code analysis for vulnerability detection.
- Security of third-party frameworks and libraries.
- Secure cryptography methods in applications.

Chapter 5: Security Testing and Software Quality Assessment.
- Penetration testing and intrusion testing.
- Security analysis of web and mobile applications.
- Assessment of software quality from a security perspective.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. "Building Secure Software: How to Avoid Security Problems the Right Way" par John Viega et Gary McGraw.
2. "The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations" par Gene Kim, Patrick Debois, John Willis, et Jez Humble.
3. "The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities" par Mark Dowd, John McDonald, et Justin Schuh.

Engineering Title: Computer Security.
Semester: 08.
TU Title:
Subject Title: Innovation and Entrepreneurship.
Credit: 1.
Coefficient: 1.

Teaching Objectives: The aim of this course is to motivate students to join the entrepreneurship world especially through the creation of viable economic and social solutions through small businesses, patents, or Startups. It continues from its predecessor.

Recommended Prior Knowledge: Entrepreneurship basics from previous course.

Course Content:
- Overview on Entrepreneurship: Business, partnerships, and Leadership.
- Innovation.
- Invention.
- Ideate.
- Generating business ideas, design.
- Identifying business opportunities.
- The tools: SWOT, PESTEL, business model canvas.
- Marketing & communication.
- Financials of the project.
- Feasibility Study & business plan, market study.
- human resources.
- How to prepare the presentation / pitch.
- Starup and innovative project labels in Algeria: how to?
- Patents: how to write and submit a patent under Algerian Law.
- Intellectual property laws and regulations in Algeria and its relationship with software (ONDA, INAPI, CATI…).

Evaluation Mode: Exam.

References:

1. Robert Papin, La création d'entreprise, Création, reprise, développement, 16e édition, Dunod, 2015.
2. Eric Ries, Lean Startup: Adoptez l'innovation continue, Éditeur : PEARSON, 2015.
3. Vincent Ydé, Créer son entreprise : du projet à la réalité, Éditeur : VUIBERT, 2009.
4. Peter Thiel and Blake Masters, Zero to One: Notes on Startups, or How to Build the Future, Crown Business, 2014.
5. Nader H. Asgary, Emerson A. Maccari, Heloisa C. Hollnagel, Ricardo L.P., Entrepreneurship, Innovation, and Sustainable Growth: Theory, Policy, and Practice [2 ed.], Routledge, 2024.

Engineering Title: Computer Security.
Semester: 08.
TU Title:
Subject Title: Multidisciplinary Project.
Credit: 4
Coefficient: 3.

Teaching Objectives: The aim of this subject is the immersion of students in the socio-economic environment by placing them in internships in companies. The project takes place during the second semester of the fourth year. It consists of the design and carrying out a small IT project which takes place in a company.

Recommended Prior Knowledge: Everything studied during the four years.

Project progress:
The project is described through precise specifications and can cover a wide variety of themes. It is proposed and supervised by a teacher from the department and must cover at least two disciplines.
The project group must be composed of 4 to 6 students. In addition to the technical content, which will consist of the application of the knowledge acquired for the implementation of the software development cycle, emphasis will be placed on the acquisition and application of organizational and relational aspects between the members of the group, the supervisor and the host company, respecting the following points:

- Analysis and division of work,
- Distribution of workloads between group members by the supervisor.
- Circulation of information between group members,
- Setting up a work schedule,
- Periodic presentations of project progress,
- Delivery of the final products set out in the project sheet,
- Writing an internship report (between 20 and 30 pages),
- Presentation of the work carried out before an examination committee.

Project Evaluation Modalities:
The project evaluation will take the form of a score out of twenty and is based on the following criteria:
- The group submits an internship report and the software accompanied by a letter of presence in the host company.
- An examination committee composed of the supervisor, a teacher from the department and possibly a representative of the host company will examine the file in the presence of the group of students.
- The final grade is delivered to each student in the group (overall grade awarded to the team or individual in the event that it is noted that the volume of work provided by the members is unequal) according to the following scale:
- The internship report is graded on 6 points.
- The software is rated on 6 points.
- The presentation and the answers to the questions are marked out of 6 points.
(The mark awarded out of 18 is equal to the average of the marks awarded by the examination committee members).
- A continuous work mark (on 2 points) is given by the supervisor. This note will in some way validate the students' attendance at periodic meetings and compliance with the set objectives.

Evaluation Mode: Exam (Project Defense).

Engineering Title: Computer Security.
Semester: 09.
TU Title:
Subject Title: Web and mobile application security.
Credit: 6.
Coefficient: 3.

Teaching Objectives: Understand the fundamental principles and concepts of secure Web browsing, Web development architecture, the main vulnerabilities and dedicated attacks on the Web, the mechanisms and best practices for developing and configuring Web applications. Understand the role of encryption in mobile application and device security and describe common scenarios in which processes encryption is applied.

Recommended Prior Knowledge: Network Security, and Digital Vulnerability Analysis.

Course Content:

Chapter 1: Vulnerabilities and Attack Methods.
- Different types of hackers.
- Hackers team organization and objectives.
- The intrusion phases.
- Vulnerability Analysis and Zero-day Vulnerabilities.
- Malicious code attacks.
- Social engineering attacks.
- Application attacks.

Chapter 2: Web security model.
- The web browser as an OS and an execution platform.
- Permission-based access control.
- Protocols, isolation, and communication.

Chapter 3: Web application security.
- OWASP - Top 10 attacks.
- Web application protection techniques.

Chapter 4: HTTPS Objectives and Problems.
- The SSL/TLS protocol: reminder.
- Strengthen security using HTTPS.
- Https problems: falsified certificate, mixed http/https traffic, etc.

Chapter 5: Content Security Policy (CSP).
- Web workers.
- Content Security Policies.
- Frame isolation (Sandboxed iFrames).

Chapter 6: Session tracking and authentication.
- How to authenticate a website.
- Secure state monitoring mechanism between client and server.
- Cookies and session integrity.

Chapter 7: XML and Web Services Security.
- Reminder about Web services.
- Security in XML.
- Overview of AJAX technology.
- Attacks on AJAX and defense mechanisms.

Chapter 8: Mobile Security.
- Mobile computing technologies.
- Overview of mobile computing security.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Mavoungou S., Kaddoum G., Taha M., and Matar G., Survey on threats and attacks on mobile networks, https://ieeexplore.ieee.org/document/8272037.
2. Papageorgiou A., Strigkos M., Politou E., Alepis E., Solanas A., and Patsakis C., Security and privacy analysis of mobile health applications: the alarming state of practice, https://ieeexplore.ieee.org/document/8272037.
3. M. Oltrogge, E. Derr, C. Stransky, Y. Acar, S. Fahl, C. Rossow, G. Pellegrino, S. Bugiel, and M. Backes, "The rise of the citizen developer: Assessing the security impact of online app generators," in 2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA, May 2018, pp. 634–647. [Online]. Available: https://doi.org/10.1109/SP.2018.00005.
4. M. Zalewski, The Tangled Web: A Guide to Securing Modern Web Applications, 1st ed. San Francisco, CA, USA: No Starch Press, 2011.

Engineering Title: Computer Security.
Semester: 09.
TU Title:
Subject Title: Emblemed Systems Security.
Credit: 6.
Coefficient: 4.

Teaching Objectives: This subject aims to present the basic concepts of embedded systems, their security, and their specificities: reduced memory size, the need to process certain information in real time, the need to discover and control new peripherals. This subject also targets the programming of microcontrollers.

Recommended Prior Knowledge: Computer architectures and machine structure.

Course Content:

1. Introduction to embedded systems.
2. Main characteristics of an embedded system.
3. SOC (System on Circuit).
   - The SOC industry.
   - IP blocks.
   - Integrated buses.
   - Design methods.
4. Constraints of an embedded operating system and cross-compilation.
5. Microcontrollers.
   - General information on microcontrollers.
   - PIC architecture: Example 16F84.
   - PIC programming.
   - Some simulations: Proteus….
6. The security of embedded systems.
   - Vulnerability analysis of embedded systems.
   - Hardware vulnerabilities.
   - Software and communication vulnerabilities.
   - Classification of attacks.
   - Types of attacks.
   - Security and supervision tools.
   - Secure development methodologies.
7. Case studies and applications.
   - Secure embedded networks examples in different fields: Agriculture, Home automation, industry, ..
   - Putting security concepts into practice in concrete cases.
8. Practical cases: Examples of smart card programming projects.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Emmanuel Grolleau, Jérôme Hugues, et al., Introduction aux systèmes embarqués temps réel - Fondamentaux et études de cas : Conception et mise en œuvre, Edition DUNOD, 2018.
2. Francine Krief, Les systèmes embarqués communicants : Mobilité, sécurité, Livre, Hermes Science Publications, 2008.
3. Philippe Louvel, Systèmes électroniques embarqués et transports, Livre, Dunod,2012
4. Daniele Lacamera, Embedded Systems Architecture: Design and write software for embedded devices to build safe and connected systems, Packt Publishing, 2023.

Engineering Title: Computer Security.
Semester: 09.
TU Title:
Subject Title: Digital Forensics.
Credit: 6.
Coefficient: 3.

Teaching Objectives: This course provides students with an understanding of the fundamental process of analyzing data collected from electronic devices (including computers, media, and other digital evidence). Students will become familiar with the appropriate techniques and tools used to secure, manipulate, and preserve digital and multimedia evidence at physical crime scenes.

Recommended Prior Knowledge: IT systems, IT networking.

Course Content:

1. Introduction.
   1.1 Management of IS security incidents.
   1.2 Evidence preservation problem.
   1.3 Incident classification: Technical failures versus natural disasters.
   1.4 Risk assessment.
   1.5 Forensics analysis Objective.
   1.6 The different approaches.
2. Dead Forensics, Live Forensics.
3. Memory analysis.
   3.1 Recovering system information.
   3.2 Retrieving process information.
   3.3 Retrieving file/directory information.
   3.4 Retrieving information from networks.
   3.5 Retrieving security information.
4. Recovery of sensitive information.
   4.1 Recovery of WiFi keys.
   4.2 Recovering browser passwords.
   4.3 Microsoft tool password recovery.
   4.5 Recovering router passwords.
5. Extracting AES keys contained in RAM.
6. Software tools (Autopsy, EnCase, etc.).

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Aitken, C.G.G., Stoney, D.A., The use of Statistics in Forensic Science, Ellis Horwood, Londres, 1991.
2. Ribaux, O., La recherche et la gestion des liens dans l'investigation criminelle : le cas particulier du cambriolage, thèse de doctorat, Institut de Police Scientifique et de Criminologie, Lausanne, 1997.
3. Robertson, B., Vignaux, G.A., Interpreting Evidence, John Wiley & Sons, Chichester, 1995.
4. Chuck Easttom, Digital Forensics, Investigation, and Response, ISSA, 2022.
5. Vashishth, Tarun, Cyber Forensics up and Running: A hands-on guide to digital forensics tools and technique, BPB Publications, 2023.
6. MUHIBULLAH. MOHAMMED, Windows Forensics Analyst Field Guide: Engage in proactive cyber defense using digital forensics techniques, Packt, 2023.

Engineering Title: Computer Security.
Semester: 09.
TU Title:
Subject Title: DevOps.
Credit: 5.
Coefficient: 3.

Teaching Objectives: Allow the student to become familiar with the concepts of software project management with DevOps, as well as its tools.

Recommended Prior Knowledge: Fundamentals of software engineering and Cloud Computing.

Course Content:

1. Introduction to DevOps: An overview of DevOps, its history, and the problems it solves.
2. Source control management: Using tools like Git for version control, managing code repositories, and collaborating on code changes.
3. Continuous Integration (CI) and Continuous Deployment (CD): How the CI/CD pipeline helps automate the development and deployment process.
4. Docker: The basics of containerization with Docker, including building Docker images, managing containers, and deploying applications using Docker.
5. Kubernetes: Kubernetes fundamentals, including deploying Kubernetes clusters, managing workloads, and scaling applications.
6. Configuration Management: Using tools like Puppet, Chef, and Ansible to manage infrastructure and application configuration.
7. Monitoring and Logging: Using tools like Nagios, ELK Stack, and Prometheus for monitoring and logging infrastructure and applications.
8. Security: The importance of security in DevOps, including securing infrastructure, managing access, and implementing secure development practices.
9. Collaboration and Communication: The importance of communication and collaboration between development and operations teams.
10. Best Practices: The course would cover DevOps best practices, including agile development, Lean principles, and DevOps culture.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Justin Domingus et John Arundel, Cloud Native DevOps with Kubernetes, 2nd Edition, O'Reilly Media, Inc., 2022.
2. Mark S. Merkow, Practical Security for Agile and DevOps, Auerbach Publications, 2022.
3. Bradley Smith, DevOps for the Desperate: A Hands-On Survival Guide, No Starch Press, Inc., 2022.
4. M. Krief, Learning DevOps: A comprehensive guide to accelerating DevOps culture adoption with Terraform, Azure DevOps, Kubernetes, and Jenkins, Packt Publishing, 2022.
5. Stephen Chin, Melissa McKay, Ixchel Ruiz, Baruch Sadogursky, DevOps Tools for Java Developers: Best Practices from Source Code to Production Containers, O'Reilly Media, 2022.
6. John Knight, Nate Swenson, The DevOps Career Handbook: The ultimate guide to pursuing a successful career in DevOps, Packt Publishing, 2022.
7. Michelle Ribeiro, Learning DevSecOps: Integrating Continuous Security Across Your Organization, O'Reilly Media, 2024.

Engineering Title: Computer Security.
Semester: 09.
TU Title:
Subject Title: Hacking Ethic.
Credit: 4.
Coefficient: 2.

Teaching Objectives: This course introduces students to the fundamentals of ethical hacking, with a focus on understanding security vulnerabilities, performing penetration tests, and implementing countermeasures. Through a combination of theoretical courses and practical exercises, students will develop the skills necessary to identify and mitigate security threats within information systems.

Recommended Prior Knowledge: Introduction to Operating Systems and Cybersecurity.

Course Content:

Chapter 1: Fundamentals of Ethical Hacking.
- 1.1. Overview of Ethical Hacking Principles and Methodologies.
- 1.2. Legal and Ethical Considerations in Penetration Testing.
- 1.3. Overview of Hacking Concepts and Hacker Classes.
- 1.4. Phases of the hacking cycle.
- 1.5. Overview of Ethical Hacking Tools.

Chapter 2: Spotting and recognition.
- 2.1. Information Gathering Techniques.
- 2.2. Network scanning and enumeration.
- 2.3. Collection of OSINT (Open-Source INTelligence).

Chapter 3: Exploration and enumeration.
- 3.1. Port exploration techniques.
- 3.2. List of services.
- 3.3. Exploring vulnerabilities with tools like Nessus and OpenVAS.

Chapter 4: System Hacking.
- 4.1. Password cracking techniques.
- 4.2. Privilege escalation.
- 4.3. Maintaining access via backdoors and rootkits.

Chapter 5: Social engineering techniques and countermeasures.
- 5.1. Introduction to Social Engineering Concepts.
- 5.2. Social engineering techniques.
- 5.3. Internal threats.
- 5.4. ID theft.
- 5.5. Countermeasures against social engineering, insider threats and identity theft.

Chapter 6: Network Attacks.
- 6.1. Packet sniffing and sniffing types.
- 6.2. Sniffing Techniques and Tools.
- 6.3. DoS/DDoS attack tools.
- 6.4. Session hijacking.

Chapter 7: Hacking Web Applications.
- 7.1. Introduction to Web Server Concepts and Attacks.
- 7.2. Attack tools and countermeasures for web servers.
- 7.3. Attack tools and countermeasures for web applications.
- 7.4. SQL Injection.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Ethical Hacking: A Hands-on Introduction to Breaking In, Daniel G. Graham, 2021.
2. Hacking: A Beginners' Guide to Computer Hacking, Basic Security, And PenetrationTesting, John Slavio, 2017.
3. Hacking: The Art of Exploitation, 2e édition, Jon Erickson, 2008.
4. Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things, Fotios Chantzis, Ioannis Stais, Paulino Calderon et al, 2021.

Engineering Title: Computer Security.
Semester: 09.
TU Title:
Subject Title: Project Management.
Credit: 1.
Coefficient: 1.

Teaching Objectives: Allow the student to understand the major issues of project management. Introduce the student to the process of organization and planning. Train the student in the application of planning processes, methods and tools. Introduce the student to project management environments.

Recommended Prior Knowledge: Project Notions.

Course Content:

1. Introduction.
   - Definition of basic concepts.
   - Notions of project and project management.
2. Project management models.
   - Models based on deliverables.
   - Risk-based models.
3. Elements of Project Management.
   - Project management issues.
   - Project management activities.
   - The project management structure.
   - Risks and project management.
4. The organization of programming teams.
   - Basic organization.
   - Support tools.
5. Elements of planning.
   - The productivity of the programmer.
   - Deadline and milestone of a project.
6. The planning process.
   - Division and coordination of activities.
   - Planning tools (scheduling of activities and allocation of resources).
   - Planning environments (eg: MSPROJECT).
7. Estimated charges, deadlines and costs.
   - Alternative options: methods.
   - The precision of the size of the programs.
   - Algorithmic estimation model.
8. Agile approach.
   - Agile principles and methods.
   - Presentation: Scrum method. XP method.

Evaluation Mode: Continuous evaluation, and exam.

References:

1. Principles of software engineering management by Tom GILB Edition Lavoisier.
2. Software Engineering: A Practitioner's Approach by Roger S Pressman.

Software Project Management in Practice by Pankaj Jalote.

Engineering Title: Computer Security.
Semester: 09.
TU Title:
Subject Title: Emerging Security Technologies.
Credit: 1.
Coefficient: 1.

Teaching Objectives: This course will cover topics like blockchain, cryptocurrency and quantum computing and other novel tech in cybersecurity. Its main goal is, thus, to explore the cutting-edge technologies of the cybersecurity world.

Recommended Prior Knowledge: Computer Security Concepts.

Course Content:

1. Introduction to Emerging Security Technologies.
   1.1. Overview of Emerging Trends in Cybersecurity.
   1.2. Zero-Trust Architecture (ZTA): Principles and Implementation.
   1.3. Manufacturer Usage Description (MUD) in Network Security.
2. Behavioral Analytics and Context-Aware Security.
   2.1. Understanding Behavioral Analytics for Threat Detection.
   2.2. Context-Aware Security: Adaptive Defense Mechanisms.
3. Advanced Encryption Techniques.
   3.1. Homomorphic Encryption: Theory and Applications.
   3.2. Cryptography in Blockchain and Cryptocurrency.
      3.2.1. Introduction to blockchain technology.
      3.2.2. Basics of blockchain cryptography.
      3.2.3. Consensus mechanisms (e.g., Proof of Work, Proof of Stake).
      3.2.4. Smart contracts and decentralized applications (DApps).
      3.2.5. Overview of cryptocurrency fundamentals.
      3.2.6. Cryptocurrency mining and transactions.
      3.2.7. Security challenges in cryptocurrency exchanges.
      3.2.8. Regulation and legal aspects of cryptocurrencies.
4. Advanced Threat Detection and Response.
   4.1. Elastic Log Monitoring for Large Data Sets.
   4.2. Extended Detection and Response (XDR) Platforms.
5. Other Novel Technologies in Cybersecurity.
   5.1. Biometric authentication and its security implications.
   5.2. Quantum Computing and its Implications for Cybersecurity.
   5.3. Future of Cybersecurity technologies and threats.

Evaluation Mode: Exam.

References:

1. Ramchandra Sharad Mangrulkar; Pallavi Vijay Chavan, Blockchain Essentials: Core Concepts and Implementations, Apress, 2024.
2. Jay Liebowitz (editor), Cryptocurrency Concepts, Technology, and Applications, Auerbach Publications, 2023.

3. Tom Madsen, Zero-trust – An Introduction, River Publishers, 2024.
4. Nirbhay Kumar Chaubey, Bhavesh B. Prajapati, Quantum Cryptography and the Future of Cyber Security, Information Science Reference, 2020.
5. Om Pal; Vinod Kumar; Rijwan Khan; Bashir Alam; Mansaf Alam, Cyber Security Using Modern Technologies: Artificial Intelligence, Blockchain and Quantum Cryptography, CRC Press ,2023.

Engineering Title: Computer Security.
Semester: 09.
TU Title:
Subject Title: Academic Communication and Research.
Credit: 1.
Coefficient: 1.

Teaching Objectives: The aim of this subject is to introduce students to the writing of scientific reports (articles, reports, theses, etc.) and the oral presentation of national and international scientific communications.

Recommended Prior Knowledge: Mastery of the used language.

Course Content:
- Principles of scientific communication.
- Publication modes: Article, Patent, Thesis, Book, Poster, Oral...
- Sources of full-text bibliographic information (the SNDL system, open access, archives, etc.).
- Structure of the different scientific publications (Articles, theses, oral presentation, etc.).
- Ethics in scientific research in Computer Science (Plagiarism, self-plagiarism, generative AI like chatGPT, etc.)
- Document preparation systems (LaTex) and bibliographic reference styles (APA, IEEEtran…etc).
- Bibliography management tools (Zotero, Mendely, EndNote, Bibtex…etc).

Evaluation Mode: Exam.

References:

1. Jean-Marie Dubois, La rédaction scientifique : mémoires et thèses : formes régulières et par articles, Estem, 2005.
2. 2. Michèle Lenoble-Pinson, La rédaction scientifique : conception, rédaction, présentation, signalétique, De Boeck Université, 1996.
3. 3.Christine Gérard, Jean Germain, Recherche bibliographique et documentaire : généralités » Faculté de philosophie et Lettres, 1985.
4. 4. Beaud, Michel. L'art de la thèse. La Découverte, 2020.
5. 5. Stefan Kottwitz, LaTeX Beginner's Guide: Create visually appealing texts, articles, and books for business and science using LaTeX, 2nd Edition, Packt Publishing, 2021.

IV- Agreements or Conventions.

Yes

No

(If yes, Transmit the Agreements and/or Conventions in the Course Paper Field).

INTENT MODEL LETTER

(In the Case of an Engineering Degree in Collaboration with a Company in the User Sector)

(Official Company Letterhead)

UBJECT: Approval of the project to launch an Engineering degree course entitled:

Dispensed to:

The company …… hereby declares its willingness to demonstrate its support for this training as a potential user of the product.

To this end, we confirm our support for this project and our role will consist of:

- Give our point of view in the development and updating of teaching programs,
- Participate in seminars organized for this purpose,
- Participate in defense juries,
- Facilitate as much as possible the reception of interns either as part of end-of-study dissertations or as part of tutored projects.

The means necessary to carry out the tasks incumbent on us to achieve these objectives will be implemented on a material and human level.

Mr. (or Madam) ……is designated as external coordinator of this project.

SIGNATURE of the legally authorized person:

FUNCTION:

Date:

OFFICIAL STAMP or COMPANY SEAL

V – Succinct Curriculum Vitae.
From the Teaching Team Mobilized for the Specialty (Internal and External).

Domain Responsible

Name and First Name:
Date and Place of Birth:
Email and Telephone:
Grade:
Establishment:
Diplomas Obtained (Graduation, Post-Graduation, etc.):

Professional Teaching Skills (Subjects taught):

Sector Responsible

Name and First Name:
Date and Place of Birth:
Email and Telephone:
Grade:
Establishment:
Diplomas Obtained (Graduation, Post-Graduation, etc.):
Professional Teaching Skills (Subjects taught, etc.):

Specialty Responsible

VI- Opinions and Visas from Administrative and Consultative Organs.

Engineering Title:

Department Head	Domain Responsible
Date, and Visa:	Date, and Visa:
Department Scientific Committee	
Date, and Visa:	
Faculty Scientific Council	
Date, and Visa:	
Faculty Dean	
Date, and Visa:	
Head of University Establishment	
Date, and Visa:	

VII – Opinion and Approval of the Regional Conference.
(Only in the Final Version Sent to the MHESR)

VIII - Opinion and Approval of the National Pedagogical Committee of the Domain.
(Only in the Final Version Sent to the MHESR).