MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Armée de Terre
Académie militaire de Saint-Cyr Coëtquidan
Direction générale de l’enseignement et de la recherche

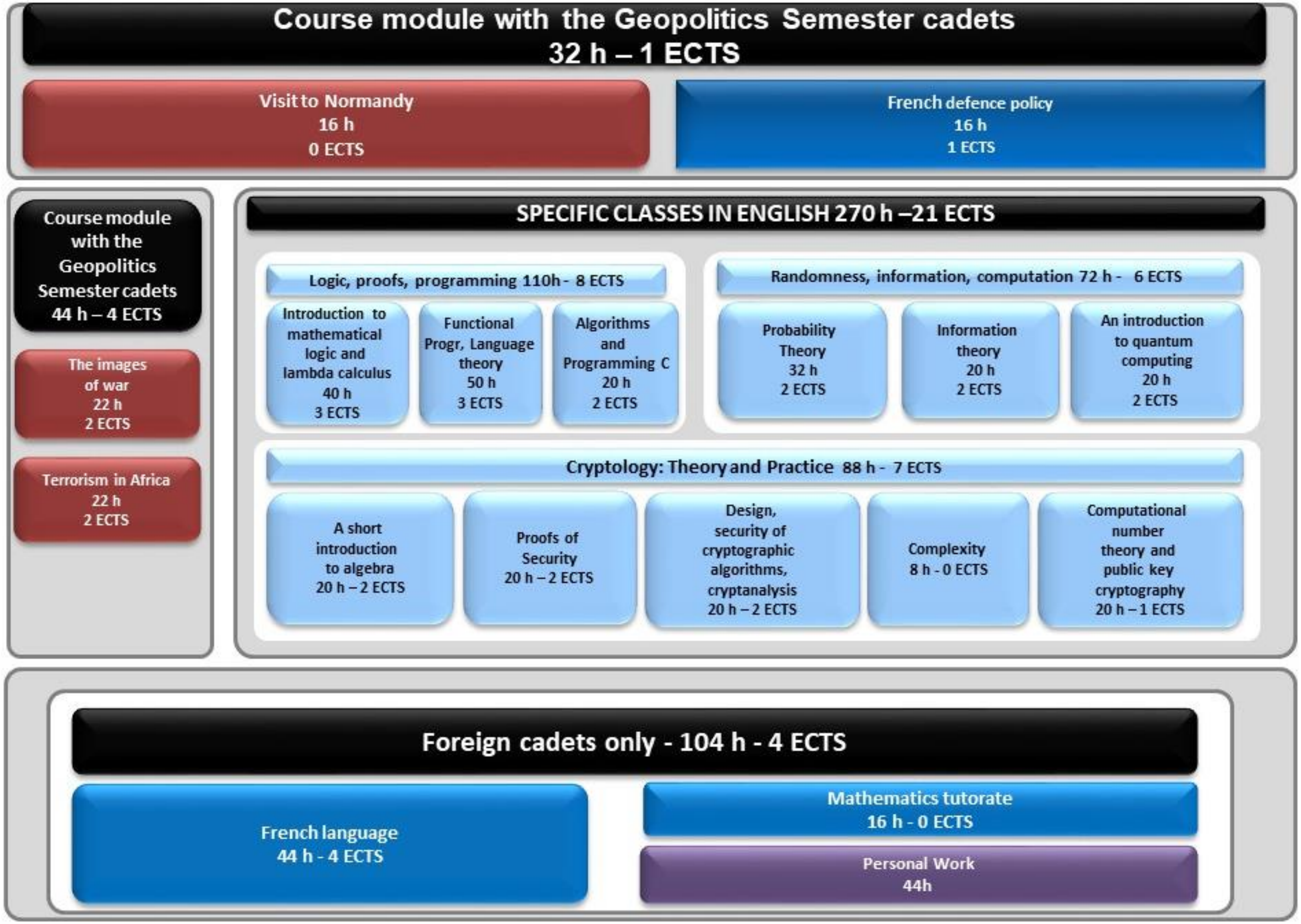
International Fall Semester 2022

Science English Language

ACADÉMIE
MILITAIRE
SAINT-CYR COËTQUIDAN

ERASMUS ID CODE	FGUER01
Contact	**Capt Aurélia WALKER** a.rispal-walker@st-cyr.terre-net.defense.gouv.fr +33 2 97 70 75 27 **Capt Samuel ARNAUD** samuel.arnaud@st-cyr.terre-net.defense.gouv.fr +33 2 97 70 79 16
Dates	Starts : 13th September 2022 Ends : 20th January 2022 Arrival date : 12th September 2022
Student Requirements	English language B1 or 785 TOEIC Undergraduate level in science
Application file	• Application form • Medical Certificate • Reduced Medical Booklet • ID or Passport scan • 1 ID photograph **Applications must be sent no later than 30th June 2022.**
Meals & Accommodation	According to EMILYO-LoD 5 (framework), accommodation, meals, and other expenses in relation to the education are free of charge for members of European Union Basic Officer Education Institutions (http://www.emilyo.eu/node/982).

Science semester in english – 30ECTS



Course module with the Geopolitics Semester cadets 32 h – 1 ECTS

Visit to Normandy
16 h
0 ECTS

French defence policy
16 h
1 ECTS

Course module with the Geopolitics Semester cadets 44 h – 4 ECTS

The images of war
22 h
2 ECTS

Terrorism in Africa
22 h
2 ECTS

SPECIFIC CLASSES IN ENGLISH 270 h –21 ECTS

Logic, proofs, programming 110h - 8 ECTS

Introduction to mathematical logic and lambda calculus
40 h
3 ECTS

Functional Progr, Language theory
50 h
3 ECTS

Algorithms and Programming C
20 h
2 ECTS

Randomness, information, computation 72 h - 6 ECTS

Probability Theory
32 h
2 ECTS

Information theory
20 h
2 ECTS

An introduction to quantum computing
20 h
2 ECTS

Cryptology: Theory and Practice 88 h - 7 ECTS

A short introduction to algebra
20 h – 2 ECTS

Proofs of Security
20 h – 2 ECTS

Design, security of cryptographic algorithms, cryptanalysis
20 h – 2 ECTS

Complexity
8 h - 0 ECTS

Computational number theory and public key cryptography
20 h – 1 ECTS

Foreign cadets only - 104 h - 4 ECTS

French language
44 h - 4 ECTS

Mathematics tutorate
16 h - 0 ECTS

Personal Work
44h

Courses Syllabus

COMMON CORE CURRICULUM

- **IMAGES OF WAR, MRS EVELYNE GOT**

The aim of the course is to discover the weight of representations on the conduct of war. What are the relations between the graphic arts and war? How have arts been used to the conduct of war? How have officers used their technical skills to represent military situations?

- **TERRORISM IN AFRICA, COL MARC HUMBERT**

Radicalization: is there a possible reversal? What makes a terrorist? De-radicalization programs. A study of the area of operations: Physical and human geography of the Sahelian strip; Nigeria, Niger, Chad and Cameroon; The Lake Chad Basin; Violence or the plague of Nigeria. Players of the drama: Boko Haram; Other terrorist organizations; The local armed forces and their auxiliaries; The population; The authorities; The international community (UNO, UNHCR, UNICEF, EU); US, UK and France; NGOs (ICRC, others). A logic leading to catastrophe: Sequence of events. 2002 to 2009: a sect is born; 2009 to 2014: growing in secret; 2014 to 2017: rise and fall of the caliphate; since 2017: no way out.

- **FRENCH DEFENSE POLICY**

The course offers an overview of the French military. The various lectures focus on the current French Defense policy (including the most recent White Paper, and ongoing operations), the organization of the three services and their capabilities. A particular emphasis is laid on the Army (organization, recent engagements, equipment, Special Forces and the Foreign Legion).

SPECIALITY COURSES IN ENGLISH

- **INTRODUCTION TO MATHEMATICAL LOGIC AND LAMBDA CALCULUS**

Logic is a typical tool that helps making decisions thanks to modelling and reasoning about situations. Logical languages allow modelling propositions as formulae and terms. Then logic gives a meaning to the formulae. Namely, natural deduction and sequent calculus provide formal and well-founded semantics to the intuitive notion of deduction. Altogether, these tools provide a framework to build and check proofs with the assistance of computer software. Since the 70s and 80s, logic and functional programming are closely entangled. On the one side the Curry-Howard correspondence states that proofs and programs are similar objects. Indeed inference rules of natural deduction or sequent calculus are similar (if not identical) to the type checking rules of functional languages. So proofs turn out to be correct-by-construction executable programs. This is an approach to build reliable, safe and secure software. On the other side, the lambda calculus defines a family of semantics for functional programming. Thanks to data immutability, this calculus is far simpler than other calculus with side effects. Functional programming thus offers a simpler setup to the introduction to program verification.

- **FUNCTIONAL PROGRAMMING**

Functional programming is paradigm and programming style that relies mainly on the concept of function. In the industry, it is mainly used in specific niches that include critical systems, one of the most famous ones being the trading system of Jane Street Capital. Since more than a decade, most of the modern programming languages like Java or C# tend to evolve, becoming multiparadigm languages that borrow several principles and features from functional programming. The popular Map Reduce parallel computing framework is also a typical system inspired by common functional programming idioms.

Functional programming relies on few simple yet powerful concepts. Functions are at the centre of the approach. As first-class values, functions can be used as parameters and return values as well, which are at the core of frameworks like Map Reduce. Data immutability avoids side effects, which improves reliability. The programming style is mainly based on recursive data structures and algorithms along with pattern matching, which typically provides equational and declarative notations. In addition to its intrinsic interest, functional programming is also a key prerequisite for the introduction to logic and lambda calculus. Indeed, the latter defines the family of semantics for functional programming, far simpler than other programming paradigms thanks to data immutability. The Curry-Howard correspondence makes functional programming an approach of choice in proof assistants.

- **PROBABILITY THEORY**

No event can be predicted with total certainty. The best we can say is how likely they are to happen, using the idea of probability. However almost nobody can deal with randomness. The intuition of almost everybody is wrong when it comes with probabilities. Even very smart mathematicians had made big mistakes on very simple random problems. The reason is that, since we are born, we are taught to think in a deterministic way. Although every aspect of our lives is random, we treat it as deterministic.

That is why we will study the probability theory in the discrete case in order to bring the cadets to reason in a probabilistic way. They should question their way of thinking. To do this, we will treat many simple cases and paradoxes. The question of the true nature of randomness will be dealt with. Indeed, although randomness appears everywhere and all the time, it seems that randomness doesn't exist (except maybe at quantum level).

Then we will focus on Markov chains. In 1907, A. Markov began the study of an important new type of chance process. During an experiment whose such a process is a model, the next outcome is affected by the current one but is not by the past ones. This type of process is called a Markov chain. It has application in every aspects of science. We will study some powerful results of such processes.

Finally, we will deal with Pseudo Random Number Generators (PRNG). Such generators create numbers that are "random" like. PNRG are central in applications such as simulations (e.g. for the Monte Carlo method) and cryptography. The question of how "random" like those PRNG are will be discussed. It will imply a statistical study. This will lead us to develop basic statistical concepts.

This 40 hours course will be organized around three distinct parts: the probability theory in the discrete case, Markov chains and the study of pseudo-random generators.

- **INFORMATION THEORY**

Since the famous Shannon paper from 1948, information theory has become the scientific field supporting the engineering of telecommunications. For instance, the capacity is the good measure of the quality of a transmission over a wireless channel, and the decoding

capability is the good measure of the quality of a telecommunication system adapted to the given transmission channel.
In cryptology also, since the Shannon paper from 1949, information theory is a fundamental domain.

- ✓ For key generation, Shannon entropy is the good measure of the average randomness of a source
- ✓ In the design of symmetric primitives, Shannon principle of diffusion (spreading randomness) is implemented through shift registers and more recently MDS matrices.
- ✓ In the analysis of symmetric primitives through statistical cryptanalysis, correlation attacks.
- ✓ In the analysis of a telecommunication chain in interception context.

During this course some essential notions of information theory will be introduced which will give the student the basics to be able to follow the course entitled DESIGN, SECURITY OF CRYPTOGRAPHIC ALGORITHMS, CRYPTANALYSIS. We will terminate the course by an example of how to use the information theory principles to reconstruct a digital telecommunication chain in a non-cooperative context.

- **AN INTRODUCTION TO QUANTUM COMPUTING**

The technological advances since the invention of the microprocessor (1970) to the most recent achievements (2015) have been exponential, leading to massive integration of transistors on a given microchip. In the last generation of microchips the individual transistors are separated by just 100 interatomic distances of the Silicium substrate. Such a pace of technological advance cannot be sustained since we shall reach soon the ineluctable barrier of atomic scale lying in the quantum realm.
Quantum computing, and more generally quantum information, instead of considering the infrangible quantum barrier as an obstacle, takes advantage of the tremendous possibilities offered by the quantum world to encode, process, transmit, and protect information by using quantum protocols. Quantum communication and cryptography are already developed in a pre-industrial level.
Quantum computing is still at a putative level; quantum processing devices have been constructed as proofs of principles. The course, after the foundational setting of quantum mechanics and there call of basic mathematical tools, will introduce q-bits, the quantum generalization of classical bits. Then the notion of quantum gates and quantum circuits will be developed. A series of quantum algorithms will then be described, culminating with the celebrated Shor’s factoring algorithm. For a physical process to be useful as a computing algorithm, its ability to correct errors is a pre-requisite. Hence the main quantum error correcting algorithms will be reviewed.
The course will end with a choice among the following topics: either some theoretical considerations concerning quantum Turing machines and quantum complexity classes or with some topics in quantum communication such as teleportation, dense coding, etc.

- **ALGORITHMS AND PROGRAMMING IN C++ AND SAGE**

The purpose of the course is to explain how to program some algorithms using C++ or Python. For example (non restrictive list) algorithms for:

- ✓ Classification: A Markov distinguisher recognizes the language of a text;
- ✓ Simulation: Generating random numbers following a given law of probability Simulating an Linear;
- ✓ Feedback Shift Register (LFSR);

- ✓ Cryptography: Hashing and collisions The primality testing (from Fermat to Rabin Miller tests);
- ✓ Factorizing big numbers (related to Rivest-Shamir-Adleman (RSA) algorithm);
- ✓ Images: Exemples of image processing.

- **A SHORT INTRODUCTION TO ALGEBRA**

Many applications from engineering and defense require some mathematical backgrounds.
For instance, in cryptography, which has become an important research area of computer science and applied mathematics, a lot of cryptosystems are based on modular arithmetic and number theory.
This course introduces some basic concepts of abstract algebra such as group, ring, and field, among others. The theory is presented and developed with the familiar examples of integers and polynomials so that the motivation is maintained. Meanwhile, the Chinese remainder theorem and the factorization problem appear naturally in this context.
As an applications of the contents provided, the widely used RSA cryptosystem is explained. Hence this course can be thought of as an introduction to the course "Computational Number. Theory and Public Key Cryptography" for which a good knowledge of the previous concepts and results is required.

- **COMPUTATIONAL NUMBER THEORY AND PUBLIC KEY CRYPTOGRAPHY**

Public key cryptography is “everywhere”. It avoids the necessity of individual key exchanges, which would be infeasible in many contexts.
We try to show some old and new systems of public key cryptography. In order to explain what makes these systems work, a well-pondered minimum of algebraic and number-theoretic background will be provided.
Objectives: Become familiar with basic notions of elementary and algorithmic number theory; understand why PKC (Public Key Cryptography) systems work, and what they are used for.

Principal Key words: Rings; computing modulo n; exponentials; RSA; hardness of factorization; finite fields; elliptic curves.

- **DESIGN, SECURITY OF CRYPTOGRAPHIC ALGORITHMS, CRYPTANALYSIS**

Symmetric primitives for cryptography form the core of cryptography from ancient times (Caesar’s cipher and Scytale) to advanced encryption standard (AES) passing through the very famous ENIGMA machine. In the modern times, a lot has been made to take into account for security not only the security of the primitive concerning the key recovery problem, but the environment in which these primitives are implemented field programmable gate array (FPGA), application specific integrated circuit (ASIC), software, radio frequency identification (RFID).
In the design of a cryptographic system it is now necessary to model the possibilities for an attacker to recover a part of information, or to impersonate the right owner of the communication. Therefore, to primitives have been added modes of operation ensuring security in different attacker models.
Another very important problem concerns, the media on which the primitives are implemented, since a study of the electric consumption can give information on what happens during the implementation.

In this course we present the principle which guides the designers to conceive new symmetric primitives, new modes of operation and review the bank of attacks that exist against the different types of primitives as well as their hardware or software implementations.

- **PROOFS OF SECURITY**

In modern cryptography, one cannot rely anymore on heuristics to declare that a system in secure. The complexity of both the systems and the attackers forces a systematic and formal approach to the notion of security.
Provable security allows us to understand, to state, and to ensure the security level of cryptographic algorithms with clear assumptions about the adversary's access to the system (i.e. the power of the adversary) and the hardness of some computational tasks (e.g. factoring).
We will show how, from a small subset of hard problems, we can build various and powerful cryptographic tools such as provably secure encryption, secure multi-party computation, or zero-knowledge proofs.

INTERNATIONAL STUDENTS SPECIFIC COURSES

- **FRENCH MODERN LANGUAGE**

This French language course is adapted according to the level of the student. Beginner courses, aim to familiarize with the basics of written and oral French language, through targeted and personalized exercises. Confirmed levels, enable students to strengthen their linguistic skills, through exercises and the study of authentic audio and written documents (films, programs, articles, books). For both levels, the aim of this course is to provide students with notions of civilization and contemporary French culture.

- **MATHEMATICS TUTORATE**

This course aims to sharpen cadets’ level in mathematics and make sure they all hold the same ground knowledge in the field.

Application file documents:

- Application Form (p.9)
- Medical Certificate (p. 10)
- Reduced Medical Booklet (p. 11 – p.12)