COURSE PLAN : « An introduction to Asymmetric Cryptography & Its Applications ”

Objective: *This course aims to provide students with a fundamental understanding of asymmetric cryptography, a cornerstone of modern cybersecurity. By the end of the course, students will be able to comprehend, analyze, and apply key concepts and techniques in asymmetric cryptography. They will gain practical skills in implementing some cryptographic algorithms (RSA) and protocols essential for securing digital communications and information systems.*

Duration:

- 15h
- When ? If possible from September 23 to September 26 or 27.
- Or: from September 17/18 to 22/23 .

Lecturer: Prof. Robert ERRA, PhD, ESIEA, Head of the Bachelor in Cybersecurity.

Prerequisites: Basics of mathematics and algorithmics, basics of Python (if possible).

Learning outcomes : Upon successful completion of this course, students will be able to:

1. Understand the principles and mathematics underlying asymmetric cryptography
2. Analyze and implement major asymmetric cryptographic algorithms in Python
3. Utilize digital signatures and authentication protocols effectively
4. Recognize and defend against common cryptographic attacks
5. Choose cryptographic techniques in various cybersecurity contexts
6. Stay informed about emerging trends and challenges in the field of cryptography

This course is essential for students pursuing a Bachelor’s degree in Cybersecurity, equipping them with the critical knowledge and skills necessary to secure digital information and communication in an increasingly connected world. For ESIEA Students it will be completed in Paris with a Project Work and another course.

Assessment and Evaluation (for ESIEA Students, in Paris):

- Lab Assignments: Practical implementation tasks to enhance hands-on skills (in Python preferably).
- A Project Work: an dividual project focusing on real-world asymmetric cryptography.

Chapter 1 (1h30) : Introduction to Cryptography

- Overview of Cryptography: Symmetric vs. Asymmetric
- Historical Background and Evolution of Cryptography
- Basic Terminologies
- Why Post Quantum Cryptography (PQC)?

Course 2 (4h30) : Mathematical Foundations : Algorithmic Algebra

- Algorithmic Number Theory:
    - Prime Numbers,

    - Modular Arithmetic
    - Fermat's and Euler's Theorems
    - Fast exponentiation
    - The Euclid and the Extended Euclid Algorithms
- From Groups to Finite Fields (Algebraic Structures)
    - The ring *Zn (n composite)*
    - The Finite Field *Zp (p prime)*

Course 3 (3h) : Asymmetric Cryptographic Algorithms

- RSA Algorithm: Key Generation, Encryption, Decryption, Security Analysis
- Diffie-Hellman Key Exchange: Concept, Process, Security Considerations
- Public Key Infrastructure (PKI)

Course 4 (2h) : Digital Signatures and Authentication

- Digital Signatures: Definition, Properties, Applications
- Digital Signature Algorithms (RSA, DSA, ECDSA)
- Authentication Protocols and Digital Certificates
- Certificate Authorities and Trust Models

Course 5 (2h00) : From Cryptography to Communication Security

- Secure Socket Layer (SSL) and Transport Layer Security (TLS)
- Pretty Good Privacy (PGP)
- Secret Sharing (the Shamir Threshold Scheme)

Course 6 (2h00) Cryptographic Attacks and Defenses [If we have time]

- How to compute RSA keys? (The Art of RSA: Past, Present, Future)
- Common Attacks on Asymmetric Cryptosystems: Man-in-the-Middle, Timing Attacks, Side-Channel Attacks
- Cryptographic Failures and Case Studies
- Best Practices for Cryptographic Security