Program of the course **HAI709I**
Fondements cryptographiques de la sécurité
Université de Montpellier, autumn 2024

In this course syllabus, the topics are grouped according to their logical connections and not chronologically. The colors are used to distinguish between the materials from the lectures by **Katharina Boudgoust** and **Andrei Romashchenko**.

I. Information-theoretic cryptography.

I.1 **Encryption with a symmetric key.** The definition of a secure (*unconditionally* secure) encryption scheme. Security of Vernam's scheme (one-time pad). A lower bound on the size of the key in a secure encryption scheme.

[Lecture notes 09/09/2024]

I.2 **Secret sharing.** The definition of a perfect secret sharing scheme. Shamir's secret sharing scheme for a threshold access structure.

[Lecture notes 16/09/2024 and 23/09/2024]

II. Algebraic tools in cryprography.

II.1 **Modular arithmetic.** The fundamental theorem of arithmetic. Arithmetic operations modulo a prime number: if p is a prime number, then for every integer number $a \neq 0 \mod p$ there exists its inverse b such that $a \cdot b = 1 \mod p$. If p is a prime number, then every polynomial of degree n with integer coefficients has at most n roots in the arithmetic $(\mathbb{Z}/p\mathbb{Z})$ (unless it is identically equal to zero modulo p).

[Lecture notes 16/09/2024 and 23/09/2024]

II.2 **Fast exponentiation algorithm.** [Lecture notes 30/10/2023]

II.3 **Finite groups.** The definition of a group. The order of a group and the order of an element in a group. In a finite group, the order of each element divides the size of this group.

II.4 **Euler's function** $\varphi(n)$. The special group $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$, in particular for a prime n and for $n = pq$ (the product of two prime numbers). The formula $x^{\varphi(n)} = 1 \mod n$ for x co-prime with n.

II.5 **Cyclic groups.** The subgroup generated by an element. The generator of a cyclic group. Existence of a generating element in $((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ for a prime p.

II.6 **The density of the set of prime numbers.** Bertrand's postulate. Chebyshev's bounds for the density of the set of prime numbers. The asymptotic law of Hadamard and de la Vallée Poussin. Lower bound for the density of prime numbers among all natural numbers with an n-bit binary expansion.

[Lecture notes 02/12/2024]

II.7 **Testing primality**. Fermat's small theorem. The Miller–Rabin algorithm for testing primality.

[Lecture notes 02/12/2024]

III. Computational complexity in cryptography.

III.1 **Computationally secure encryption scheme with a symmetric key.** Polynomial-time algorithms, negligibly small probability of error. The formal definition of a scheme secure against an adversary computable in polynomial time (an attack where the opponent may choose two clear messages, the sender encrypts one of them, and then the opponent tries to guess which message was encrypted).

[Lecture notes 23/09/2024]

III.2 **Pseudo-random generators.** The formal definition and basic properties of a pseudo-random generator. A construction of a computationally secure encryption scheme using a pseudo-random generator.

[Lecture notes 30/10/2023, 07/10/2024, and 14/10/2024]

III.3 **Semantic security** of a computationally secure encryption scheme: given the encrypted messages, the adversary cannot learn any substantial information on the encrypted message. Examples of attacks that fail due to the definition of security against an adversary computable in polynomial time (e.g., given the encrypted messages, the adversary cannot learn the 1st bit of the clear message with a probability significantly greater than $1/2$).

[Lecture notes 07/10/2024]

III.4 **Non-invertible functions:** weak and strong one way functions, a one-way function with a hard-core predicate. A strong one-way function can be constructed given a weak one-way function. A one-way function with a hard-core predicate can be constructed from one-way function. A pseudo-random generator can be constructed from a length-preserving one-way permutation.

The functions $[p, q] \mapsto p \cdot q$ and $[x, g, n] \mapsto [g^x \mod n, n]$ as possible weak one-way function.

[Lecture notes 09/12/2024]

III.5 **Bit commitment and applications:** two cryptographic protocols for the game *heads and tails*. Zero-knowledge proof for 3-coloring of a graph.

[Lecture notes 14/10/2024 and 09/12/2024]

IV Public-Key Revolution

IV.1 **Hardness assumptions.** The discrete logarithm problem. The Diffie-Hellman problem, both as computational and decisional problem. The factorization problem. The RSA problem. Some relations among them.

IV.2 **Key exchange protocol.** The definition of a correct and secure key exchange protocol. The example of the Diffie–Hellman key exchange protocol, based on DDH.

IV.3 **Public-key encryption scheme.** The definition of a correct and IND-CPA secure public-key encryption scheme. The example of the ElGamal encryption scheme. The example of the RSA encryption scheme (not IND-CPA secure).

IV.4 **Digital signature scheme.** The definition of a correct and EUF-CMA secure digital signature scheme. The example of the RSA encryption scheme (not EUF-CMA secure). The secure variant using a hash function modeled as a random oracle.

References

[1] J. Katz, Y. Lindell. Introduction to modern cryptography CRC Press, 2021.

[2] B. Martin. Codage, cryptologie et applications. PPUR, 2004.

[3] H. Tyagi and S. Watanabe. Information-theoretic cryptography. Cambridge Univ. Press, 2023.

[4] Th. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001.