Program of the course **HAI709I**

Fondements cryptographiques de la sécurité

Université de Montpellier, autumn 2023

I. Algebraic tools.

I.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 has at most n roots in the arithmetic $(\mathbb{Z}/p\mathbb{Z})$.

I.2 **Finite groups.** The definition of a group. The order of an element in a group. In a finite group, the order of each element divides the size of this group.

I.3 **Euler's function** $\varphi(n)$. The sizes groupes $((\mathbb{Z}/n\mathbb{Z})^{\times}, \cdot)$ 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.

I.4 **Generating element** in a group. Existence of a generating element in $((\mathbb{Z}/p\mathbb{Z})^{\times}, \cdot)$ for a prime p.

I.5 **Fast exponentiation algorithm.**

II. Information-theoretic cryptography.

II.1 **Encryption with a symmetric key.** The definition of a 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.

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

II.3 **Shannon's entropy.** Optimal length of a code for a message of length N over an m-letters alphabet with know frequencies of letters.

II.4 **Basic properties of Shannon's entropy.** for a random variable X distributed in a set of cardinality n it holds $0 \leq H(X) \leq \log_2 n$; for all jointly distributed (X, Y) we have $H(X, Y) \leq H(X) + H(Y)$ and $H(X, Y) = H(X \mid Y) + H(Y)$.

II.5 **Entropic bound for the size of a secret key :** in a secure encryption scheme, the Shannon entropy of the secret key cannot be less than the Shannon entropy of the random clear message.

III. Computational complexity in cryptography.

III.1 **Computationally secure** encryption scheme with a symmetric key : the formal definition.

III.2 **Pseudo-random generators.** A construction of a computationally secure encryption scheme using a pseudo-random generator.

III.3 **Semantic security** of a computationally secure encryption scheme.

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 from a weak one-way function. The construction of Goldreich–Levin of a hard-core predicate. A pseudo-random generator from a one-way function.

III.5 **Hardness of integer factorisation :** the functions $[p, q] \mapsto p \cdot q$ and $[x, n] \mapsto [x^2 \mod n, n]$ as possible weak one-way function. Fast algorithm for square root modulo n gives an algorithm of fast factorisation of the integer number n (the case when n is a product of two prime numbers) and, respectively, hardness of factorisation implies hardness of square root.

III.6 **Quadratic residues modulo n.** The pseudo-random generator of Blum–Blum–Shub.

III.7 **Bit commitment :** two cryptographic protocols for the game *heads and tails.*

III.8 **The Diffie–Hellman key exchange protocol.** The hypothesis of hardness of the problem of descrete logarithm.

III.9 **Asymmetric encryption scheme RSA.** The scheme of electronic signature based on RSA.

III.10 **Cryptographic hash functions.** The definition of collision resistant hash functions. Hashing and electronic signature.

III.11 **Zero-knowledge proof** for 3-coloring of a graph.

Références

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

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

[3] V. V. Yaschenko, Cryptography : An Introduction, AMS, 2002.

[4] Th. M. Cover and J. A. Thomas. Elements of Information Theory. Cover, Thomas M. Elements of information theory. John Wiley & Sons. 1999.

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