Course Title: Mathematics for Cryptography	**Number of Units:** 1
SSD : INF01	**CFU:** 6
Course aims: the purpose of the course is to introduce the student to number theoretic topics, both ancient and very modern, which are at the center of interest in contemporary cryptography, especially in the most known public key cryptosystems such as RSA; an algorithmic approach is taken, emphasizing estimates of the efficiency of the techniques that arise from the theory.	
Course Description: Elementary Number Theory: notation and basic properties; divisibility and the Euclidean algorithm; congruences; modular arithmetic; basic arithmetic functions (the Euler totient function, the Moebius function); the Chinese Remainder Theorem with some applications; polynomial congruences modulo a prime number (the Lagrange Theorem); quadratic residues; the Legendre symbol; the Jacobi symbol; quadratic reciprocity law; finite fields Computational Number Theory: times estimates for doing elementary arithmetic; basic notions on computational complexity and classification of the algorithms; estimating the number of bit operations needed to perform some number theoretic tasks by computer, such as the Euclidean algorithm, the repeated squaring method and the Jacobi algorithm; the discrete logarithm problem; the distribution of prime numbers with applications to the computational complexity Primality: pseudoprimes (the Fermat pseudoprimes, the Euler pseudoprimes, the strong pseudoprimes); Carmichel numbers; primality test (Solovay-Strassen and Miller -Rabin); times estimates for primality tests Factoring: basic facts on the factoring problem; the Erathostenes method; the Fermat method; the Pollard method; smooth numbers; the quadratic sieve method; some notes on the Number Field Sieve. The arithmetic of the elliptic curves: basic facts on the elliptic curves; primality test; the Lenstra factorization method; the discrete logarithm problem on the elliptic curves. Cryptography: some simple cryptosystems; symmetric keys; public key cryptography; the Diffie-Helmann problem; the RSA protocol; elliptic curve cryptosystems; cryptanalysis	
Assumed Background: Undergraduate level	
Assessment methods: written dissertation and oral colloquium	