|  |
| --- |
| ***CR510 - CRITTOSISTEMI ELLITTICI*** |

|  |  |
| --- | --- |
| |  | | --- | | **Obiettivi Formativi del corso** | |
| |  | | --- | | ACQUISIRE UNA CONOSCENZA DI BASE DEI CONCETTI E METODI MATEMATICI RELATIVI ALLA TEORIA DELLE CURVE ELLITTICHE DEFINITE SU CAMPI FINITE E LE LORO APPLICAZIONI NEL CAMPO DELLA CRITTOGRAFIA. | |
| |  | | --- | | A description... | |
| |  | | --- | | **Programma del Corso** | |
| |  | | --- | | L’equazione di Weierstrass, La struttura di gruppo dei punti razionali, l' invariante  j di una curva ellittica, curve ellittiche in caratteristica 2, Endomorfismi. Nucleo degli endomorfismi separabili. Punti di torsione, Polinomi di divisione. L’accoppiamento di Weil. L’endomorfismo di Frobenius e sue proprietà. Enunciato del Teorema di Waterhouse e di Ruck. Il Teorema di Hasse. Polinomio caratteristico dell’endomorfismo di Frobenius. Curve su sottocampi, L’algoritmo ”Baby Step, Giant  Step” di Shanks. L’algoritmo di Schoof. Attacco MOV. Attacco su  curve anomale. Crittosistemi sulle curve ellittiche basati sul problema della fattorizzazione. Fattorizzazione di numeri interi utilizzando le curve ellittiche. | |
| |  | | --- | | A description... | |
| |  | | --- | | **Testi di Riferimento** | |
| |  | | --- | | *Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart,*  **Advances in elliptic curve cryptography**, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.  *Joseph H. Silverman and John Tate,*  **Rational points on elliptic curves**, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.  *Lawrence C. Washington,*  **Elliptic curves: Number theory and cryptography**, 2nd ED. Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2008. | |

|  |
| --- |
| ***CR510 – ELLIPTIC CRYPTOSYSTEMS*** |

|  |
| --- |
| **Training objectives of the course** |

ACQUIRE GOOD KNOWLEDGE OF THE CONCEPTS AND MATHEMATICAL METHODS OF ELLIPTIC CURVES DEFINED OVER FINITE FIELDS E THEIR APPLICATION IN THE FIELDS OF CRYPTOGRAPHY.

|  |
| --- |
| **Course programme** |

The Weierstrass equation, the structure of the group of rational points, the j-invariant of an elliptic curve, elliptic curves in characteristic 2, endomorphisms. Kernel of a separable endomorphism. Torsion points, division polynomials. The Weil pairing. The Frobenius endomorphism and its properties. Statement of Waterhouse and Ruck Theorems. Hasse's theorem. Characteristic polynomial of Frobenius Endomorphism. Subfields curves, the "Baby Step, Giant Step " Shanks' algorithm. Schoof's algorithm. MOV attack. Cryptosystems based on elliptic curve factorization problem. Factorization of integers using elliptic curves.

|  |
| --- |
| **Reference Texts** |

*Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart,*

**Advances in elliptic curve cryptography**, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.

*Joseph H. Silverman and John Tate,*

**Rational points on elliptic curves**, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

*Lawrence C. Washington,*

**Elliptic curves: Number theory and cryptography**, 2nd ED. Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2008.