Programma del corso di Crittografia
aa 2010-11

Numeri primi – Congruenze – Teorema cinese dei resti - Elementi invertibili in Z_n. Piccolo teorema di Fermat - Teorema di Wilson – Funzione ϕ e Teorema di Eulero – esistenza di radici primitive modulo n e struttura del gruppo degli invertibili in Z_n - scrittura di numeri naturali in base b – operazioni - residui quadratici modulo un primo – simboli di Legendre e Jacobi – legge di reciprocita' quadratica (senza dimostrazione) – algoritmo per l'estrazione di radice modulo un primo – campi finiti – struttura del gruppo degli invertibili in un campo finito - logaritmo discreto – Algoritmo di Massey Omura per il calcolo del logaritmo discreto – Baby steps-giant steps
Analisi del costo temporale delle operazioni
Introduzione alle curve ellittiche – curve ellittiche su campi finiti e modulo n – logaritmo discreto sulle curve ellittiche (algoritmo di Silver Pohlig Hellman)
Test di primalità correlati ai teorema di Femat e di Wilson – test di Lucas – numeri di Fermat, Mersenne e Carmichael– pseudoprimi e pseudoprimi di Eulero – test di primalità probabilistici (Fermat, Solovay Strassen, Miller Rabin) – AKS
Algoritmo di fattorizzazione di Fermat – metodo delle basi di fattorizzazione – Algoritmo di Lenstra
Sistemi crittografici e chiavi – sistemi simmetrici e asimmetrici – Cifrari per traslazione – cifrari affini – cifrari affini per digrafi – crittoanalisi - analisi delle frequenze – RSA- El Gamal – firma digitale standard – crittografia sulle curve ellittiche