CR1 Crittografia a chiave pubblica

A.A. 2007/2008

Prof. Francesco Pappalardi

1. Argomenti di Teoria dei numeri elementare. Il concetto di operazione bit tipo somma o sottrazione. Stima del numero di operazioni bit (tempo macchina) per eseguire le operazioni fondamentali. Algoritmi che convergono in tempo esponenziale o polinomiale. Divisibilità. Algoritmo di Euclide (identitá di Bezout) e suo tempo di esecuzione. Congruenze. Teorema cinese dei resti. L'algoritmo dei quadrati successivi.

2. RSA. Formulazione dell'algoritmo e sua analisi del suo tempo di esecuzione. Esempi concreti non realistici. Distribuzione di Numeri primi. Il Teorema di Chebicev. Costruzione di numeri primi (grandi): Simboli di Legendre e simboli di Jacobi. Legge di reciprocità quadratica generale (senza dimostrazione) – algoritmo polinomiale per il calcolo del simbolo di Jacobi. Numeri di Carmichael. Pseudo–primi, pseudo–primi di Eulero e pseudo–primi forti. Algoritmi Montecarlo e Las–Vegas. Il test di Solovay–Strassen e quello di Miller–Rabin. Teorema di Pocklington e certificazione di primalità. Fattorizzazione alla Fermat. Metodo ρ di Pollard di Fattorizzazione.

3. Campi finiti. Fatti fondamentali di teoria dei campi. Teorema dell'elemento primitivo in un campo finito. Esistenza e unicità dei campi finiti (campi di spezzamento). Esempi. Polinomi irriducibili e primitivi. Enumerazione dei polinomi irriducibili e primitivi. Aritmetica in tempo polinomiale sui campi finiti. Test deterministici di irriducibilità in campi finiti.

4. Logaritmi discreti. Il problema del logaritmo discreto in un gruppo ciclico astratto. Metodo di Diffie Hellman per lo scambio delle chiavi. Metodo di Massey Omura per la trasmissione dei messaggi. Il crittositema di ElGamal. Firma digitale DSS. Esempi. Algoritmi per il calcolo dei logaritmi discreti nei campi finiti: L' algoritmo di Shanks Baby Steps Giant Steps, l'algoritmo Pohlig - Hellman.

5. Altri Algoritmi. Crittosistemi Ellittici: Generalità sulle curve ellittiche senza dimostrazioni, definizione di addizione sui punti razionali di una curva ellittica. Teorema di Struttura del gruppo dei punti razionali di una curva ellittica su un campo campo finito (solo enunciato), Teorema di Hasse (solo enunciato).

Testi consigliati

[1] Neal Koblitz, *A Course in Number Theory and Cryptography*. Springer, (1994). Graduate Texts in Mathematics, No 114.
[2] Douglas R. Stinson, *Cryptography: Theory and Practice*. CRC Pr, (1995).
[3] Rudolf Lidl, Harald Niederreiter, *Finite Fields*. Cambridge University Press, (1997).
[4] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *Pari–GP (2.014)*. http://pari.home.ml.org, (1998).
[5] Richard Crandall, Carl Pomerance, *Prime numbers, a computational Perspective*. Springer, (2001).
[6] F. Pappalardi, *NOTE DI CRITTOGRAFIA A CHIAVE PUBBLICA* . Fascicolo 1. Prerequisiti di Matematica, (2003).

Modalità d'esame

- valutazione in itinere ("esoneri")		■ SI	□ NO
- esame finale	scritto	■ SI	□ NO
	orale	■ SI	□ NO
- altre prove di valutazione del profitto (meglio descritte sotto)		□ SI	■ NO