CR1 Crittografia a chiave pubblica

A.A. 2001/2002

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 Esempi concreti non realistici. 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. Successioni di Lucas. Test di primalità di Lucas–Lehmer. Teorema di Pocklington e certificazione di primalità. Errori nell'implementare RSA: Modulo RSA con un fattore troppo piccolo, modulo RSA con fattori troppo vicini, Pubblicazione esponente di decodifica implica fattorizzazione del modulo RSA. Il metodo di fattorizzazione ρ di Pollard. Il metodo $p-1$.

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. Algoritmo di Berlekamp per la fattorizzazione di polinomi.

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 con Massey Omura. Esempi. Algoritmi per il calcolo dei logaritmi discreti nei campi finiti: L' algoritmo di Shanks, L'algoritmo Pohlig - Hellman.

5. Altri Algoritmi. Crittosistemi Ellittici: Generalità sulle curve ellittiche, definizione di addizione sui punti razionali di una curva ellittica, Il gruppo di Mordell–Weil, Teorema di Struttura del gruppo di Mordell Weil di una curva ellittica su un campo campo finito (solo enunciato), Teorema di Hasse (solo enunciato), esempio. Il crittosistema di ElGamal su $E(\mathbf{F_p})$. Il crittosistema di Menezes–Vanstone.

6. Sistema Pari GP. Programmazione nel Sistema Pari per calcolare con numeri a precisione arbitraria, Implementazione degli algoritmi analizzati durante il corso.

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*. Versione provvisoria, (2002).

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

Sono proposti una serie di esercizi da svolgere a casa durante il corso.