MA2 Matematica Applicata: Laboratorio 2

A.A. 1999/2000

Prof. Francesco Pappalardi

Crittografia a chiave pubblica

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. Esempi di fattorizzazione.

2. RSA. L'algoritmo di Adleman, Shamir e Rivest.

Formulazione dell'algoritmo e analisi del suo tempo di esecuzione. 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. pseudo–primi di Eulero e pseudo–primi forti. Algoritmi montecarlo. Il test di Solovay–Strassen. il test di Miller–Rabin. Accortezza nell'implementazione di RSA: Modulo RSA con un fattore troppo piccolo, Modulo RSA con fattori troppo vicini, Pubblicazione del'esponente di decodifica – Algoritmi Las–Vegas per fattorizzazione del Modulo RSA. Il crittosistema di Rabin. Il metodo di fattorizzazione $p-1$.

3. DES.

L'algoritmo a chiave privata Data Encryption Standard. Modalità di uso del DES (triplo DES, ECB, CBC, CFB): cenni.

4. 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. Esempi. Fattorizzazione nell'anello dei polinomi $\mathbf{F}_p[x]$: Gli algoritmi di Berlekamp (campi piccoli e campi grandi), Esempi, calcolo delle radici dei polinomi.

5. Logaritmi discreti.

Funzioni a trappola. 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. Esempi. Algoritmi per il calcolo dei logaritmi discreti nei campi finiti: L' algoritmo di Shanks, L'algoritmo di Pohlig–Hellman, esempi.

6. Altri Algoritmi.

Metodo dello zainetto, Crittosistema di Merkle–Hellman (esempio), Crittosistema di Chor–Rivest. 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.

7. Sistema Pari GP. Facoltativo: Rudimenti del Sistema Pari per cacolare con numeri a precisione arbitraria e campi finiti.

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).

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

Oltre agli 8 compiti svoltisi durante il corso (oppure oltre allo scritto finale), gli studenti che aspirano ad alzare il loro voto di due punti possono realizzare:

1. Una simulazione del Crittosistema di ElGamal in un campo finito che non sia un campo primo e abbia ordine $\geq 3^4$.
2. Una simulazione del Crittosistema di Rivest–Chor in un campo finito del tipo $\mathbf{F}_{p^n}$ con $p, n \geq 5$