

MA2 Matematica Applicata: Laboratorio 2

A.A. 2000/2001

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 (identità 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. Numeri di Carmichael. Pseudo-primi, pseudo-primi di Eulero e pseudo-primi forti. Algoritmi montecarlo. Il test di Solovay-Strassen. il test di Miller-Rabin. Certificazione di primalità. Teorema di Pocklington. Accortezza nell'implementazione di RSA: Modulo RSA con un fattore troppo piccolo, Modulo RSA con fattori troppo vicini, Pubblicazione dell'esponente di decodifica – Algoritmi Las-Vegas per fattorizzazione del Modulo RSA. Firme digitali. Il crittosistema di Rabin. Il metodo di fattorizzazione $p - 1$. Crivello quadratico.

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.

5. 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 crittosistema di ElGamal. Firma digitale con Massey Omura. Esempi. Algoritmi per il calcolo dei logaritmi discreti nei campi finiti: L' algoritmo di Shanks.

6. 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 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. Rudimenti del Sistema Pari per calcolare con numeri a precisione arbitraria.

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”)		<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO
- esame finale	scritto	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO
	orale	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO
- altre prove di valutazione del profitto (meglio descritte sotto)		<input type="checkbox"/> SI	<input checked="" type="checkbox"/> NO