CR1 Crittografia 1

A.A. 2003/2004

Dott.ssa Francesca Tartarone

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. L'algoritmo dei quadrati successivi.

2. RSA.

L'algoritmo di Adleman, Shamir e Rivest. Formulazione dell'algoritmo e sua analisi Esempi concreti non realistici. Distribuzione di Numeri primi. Il Teorema di Chebicev. 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 e quello di Miller–Rabin. Fattorizzazione di un intero: metodo ρ di Pollard, metodo $p-1$ di Pollard.

3. Campi finiti.

Fatti fondamentali di teoria dei campi. Teorema dell'elemento primitivo in un campo finito. Costruzione di un campo finito e sua unicità. Esempi. Polinomi irriducibili e primitivi. Enumerazione dei polinomi irriducibili e primitivi. Aritmetica in tempo polinomiale sui campi finiti. Test deterministici di irriducibilità dei polinomi nei campi finiti. Algoritmo di Berlekamp per la fattorizzazione di polinomi in un campo finito.

4. Logaritmi discreti.

Il problema del logaritmo discreto in un gruppo ciclico astratto. Algoritmi per il calcolo dei logaritmi discreti nei campi finiti: l' Algoritmo di Shanks, l'Algoritmo di Pohlig - Hellman ed il Metodo del Calcolo dell'Indice. Il crittositema di ElGamal. Metodo di Massey Omura per la trasmissione dei messaggi. Metodo di Diffie Hellman per lo scambio delle chiavi. Schemi di firma digitale: El-Gamal, DSS. Esempi.

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] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications.*. CRC Press, Boca Raton, FL, (1997).

[4] F. Pappalardi, *NOTE DI CRITTOGRAFIA A CHIAVE PUBBLICA* . Fascicolo 1. Prerequisiti di Matematica, (2003).

[5] A. Susa, *NOTE DI CRITTOGRAFIA A CHIAVE PUBBLICA* . Fascicolo 3. Campi finiti, Logaritmi discreti e crittosistemi derivati., (2003).

Bibliografia supplementare

[6] Richard Crandall, Carl Pomerance, *Prime numbers, a computational Perspective*. Springer, (2001).

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