

# CR1 Crittografia 1

## A.A. 2006/2007

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. Attacchi al crittosistema RSA (esponenti di cifratura e decifratura troppo piccoli, attacco ciclico, attacco del punto fisso, modulo comune). Frazioni continue e attacco di Weiner. Richiami sulle congruenze quadratiche e i simboli di Legendre e Jacobi. Algoritmo polinomiale per il calcolo del simbolo di Jacobi. Crittosistema di Rabin: descrizione, sicurezza ed esempi. Test di primalità basati sulla condizione di Fermat. Test di Pocklington. Pseudo-primalità di Eulero e pseudo-primalità forte. Numeri di Carmichael: caratterizzazione e prime proprietà. Algoritmi Montecarlo. Test di Solovay-Strassen. Numeri pseudo-primi forti. Test di Miller-Rabin. Fattorizzazione di un intero: metodo  $\rho$  di Pollard, metodo  $p - 1$  di Pollard, fattorizzazione alla Fermat.

### 3. Campi finiti.

Fondamenti di teoria dei campi. 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. Problema di Diffie Hellman. Scambio di chiavi di Diffie Hellman sui campi finiti. Crittosistemi di El Gamal e Massey Omura sui campi finiti. 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. Schemi di firma digitale: El-Gamal. Esempi.

## TESTI CONSIGLIATI

- [1] W.M. BALDONI, C. CILIBERTO, G.M. PIACENTINI, *Aritmetica, crittografia e codici*. Springer Verlag, (2006).
- [2] LANGUASCO ALESSANDRO, ZACCAGNINI ALESSANDRO, *Introduzione alla crittografia. Algoritmi, protocolli, sicurezza informatica*. Hoephli, (2004). Hoepli informatica.

## BIBLIOGRAFIA SUPPLEMENTARE

- [3] RICHARD CRANDALL, CARL POMERANCE, *Prime numbers, a computational Perspective*. Springer, (2001).
- [4] NEAL KOBLITZ, *A Course in Number Theory and Cryptography*. Springer, (1994). Graduate Texts in Mathematics, No 114.
- [5] 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).

## 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