MA2 Matematica Applicata: Laboratorio 2

A.A. 1998/1999

Prof. Alberto Berretti e Prof. Francesco Pappalardi

Introduzione alla Crittografia

1. Terminologia e Crittografia classica.

Algoritmi di sostituzione e trasposizione. Algoritmi di XOR, Vigenere, Vernam. Teoria di Shannon, entropia.

2. Introduzione ai protocolli crittografici.

Algoritmi a chiave privata e a chiave pubblica. Firma digitale e funzioni di Hash. Considerazioni sulla lunghezza delle chiavi.

3. Algoritmi a chiave privata (o simmetrica).

DES (Data Encryption Standard). Modalità di uso del DES e degli altri algoritmi a chiave privata: triplo DES, ECB, CBC, CFB. Algoritmi a blocchi vs. algoritmi di crittografia di flussi (stream ciphers). RC4 (ARCFOUR).

4. 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.

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

Formulazione dell'algoritmo e analisi del suo tempo di esecuzione. Esempi concreti non realistici. Metodi di implementazione pratica. Errori frequenti nell'implementazione di RSA: Modulo RSA con un fattore troppo piccolo, Modulo RSA con fattori troppo vicini, Pubblicazione della chiave di decodifica. Uso di RSA per la firma digitale.

6. Campi finiti.

Fatti fondamentali di teoria dei campi. Teorema dell'elemento generatore. Esistenza e unicità dei campi finiti (campi di spezzamento). Polinomi irriducibili e primitivi. Aritmetica in tempo polinomiale sui campi finiti. Esempi.

7. Logaritmi discreti.

Funzioni a trappola. Metodo di Diffie Hellman per lo scambio delle chiavi. Metodo di Massey Omura per la trasmissione dei messaggi. Il crittositema di ElGamal. DSS (Digital Signature Standard). Algoritmi per il calcolo dei logaritmi discreti nei campi finiti.

8. Altri Algoritmi.

Metodo dello zainetto. Dimostrazioni a conoscenza zero. isomorfismi di grafi. prove di identitá a conoscenza zero. Algoritmo di Feige-Fiat-Shamir.

9. Aspetti pratici.

Framework X.509. Autenticità certificazioni. PGP.

Testi consigliati

[1] Bruce Schneier, *Applied Criptography*. John Wiley & Sons, Inc., (1996). seconda edizione.

[2] Neal Koblitz, *A Course in Number Theory and Cryptography*. Springer, (1994). Graduate Texts in Mathematics, No 114.

[3] Douglas R. Stinson, *Cryptography: Theory and Practice*. CRC Pr, (1995).

Bibliografia supplementare

[4] Jan C. A. van der Lubbe, *Basic Mathods of Cryptography*. Cambridge University Press, (1988).

[5] Neal Koblitz, *Algebraic Aspects of Cryptography*. Springer, (1998). Algorithms and Computation in Mathematics, Vol 3.

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

Gli studenti sono invitati a svolgere un progetto che consiste nella redazione di un programma con un linguaggio di programmazione a scelta che implementi un algoritmo tra quelli svolti durante il corso.