CR410 – Crittografia a chiave pubblica

Programma - a.a. 2025/2026

Introduzione alla crittografia. Cenni storici; crittografia, crittoanalisi e crittologia. Definizione di crittosistema, cifratura e decifratura. Cifrari classici ed esempi di crittoanalisi. Principio di Kerckhoffs. Tipi di attacco: ciphertext-only, known-plaintext, chosen-plaintext, chosen-ciphertext. Crittografia simmetrica e problema della distribuzione delle chiavi. One-time pad e segretezza perfetta di Shannon.

Crittografia a chiave pubblica e complessità. Idea della crittografia a chiave pubblica; funzioni unidirezionali e trapdoor. Cenni di teoria della complessità: lunghezza dell'input, operazioni bit, complessità polinomiale ed esponenziale, classi P e NP. Algoritmo di Euclide, identità di Bézout e algoritmo esteso; complessità dell'algoritmo di Euclide, successione di Fibonacci e teorema di Lamé. Problema dello zaino, sequenze supercrescenti, crittosistema di Merkle–Hellman e sua vulnerabilità. Crittosistemi ibridi.

Aritmetica modulare e RSA. Funzione di Eulero; teoremi di Fermat ed Eulero–Fermat. Esponenziazione modulare e algoritmo square-and-multiply. Numeri di Mersenne e di Fermat. Crittosistema RSA: generazione delle chiavi, cifratura, decifratura e correttezza, anche per messaggi non coprimi con il modulo; uso del teorema cinese dei resti. Problema RSA, rapporto fra inversione RSA e fattorizzazione, funzioni trapdoor.

Test di primalità. Pseudoprimi di Fermat e numeri di Carmichael. Simboli di Legendre e Jacobi; criterio di Eulero. Test di Solovay–Strassen e pseudoprimi di Eulero–Jacobi. Test di Miller–Rabin e radici non banali dell'unità modulo un composto.

Attacchi a RSA, radici modulari e crittosistemi collegati. Scelta dei parametri RSA e vulnerabilità dovute a scelte deboli. Attacchi con esponente piccolo, broadcast/Håstad e Wiener mediante frazioni continue. Radici quadrate modulo $N = pq$ e teorema cinese dei resti. Equivalenza probabilistica fra estrazione di radici quadrate modulo N e fattorizzazione. Crittosistema di Rabin, ambiguità in decifratura e ridondanza. Crittosistema di Goldwasser–Micali e problema della residuosità quadratica.

Algoritmi di fattorizzazione. Divisione per tentativi e complessità in funzione della lunghezza dell'input. Metodo di Fermat e fattorizzazione come differenza di quadrati. Algoritmi special-purpose e general-purpose. Algoritmo $p-1$ di Pollard; numeri lisci e power-smooth. Algoritmo ρ di Pollard, iterazioni modulari, ricerca di cicli e metodo di Floyd. Metodo dei quadrati casuali di Dixon, basi di fattori, numeri lisci e algebra lineare su $\mathbb{F}_2$.

Logaritmo discreto e crittosistemi basati sul DLP. Gruppi ciclici e problema del logaritmo discreto. Algoritmi baby-step giant-step, ρ di Pollard, Pohlig–Hellman e index calculus. Scambio della chiave di Diffie–Hellman. Crittosistema di ElGamal.

Firma digitale. Requisiti e struttura di uno schema di firma digitale. Firma RSA e firma ElGamal. Funzioni hash e loro uso nelle firme digitali.

Protocolli crittografici e altri argomenti. Protocolli crittografici per problemi specifici. Condivisione di segreti. Introduzione alle prove a conoscenza zero. Cenni di crittografia post-quantum ed esempi di sistemi code-based e lattice-based, tra cui McEliece, GGH e NTRU.

Testi di riferimento. A. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo, *Aritmetica, crittografia e codici*; D. R. Stinson, M. Paterson, *Cryptography: Theory and Practice*; J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*; A. Languasco, A. Zaccagnini, *Manuale di crittografia*; J. Katz, Y. Lindell, *Introduction to Modern Cryptography*.