Programma del corso di Elementi di Crittografia
per l'a.a. 2009/10
(Francesca Merola)

- Introduzione alla crittografia. Cenni storici. Definizione di crittosistema. Cifrari classici: cifrari additivi, cifrari a sostituzione, cifrari affini, cifrari a trasposizione, cifrario di Vigenère, cifrario di Hill, cifrari affini lineari.

- Introduzione alla crittoanalisi. Crittoanalisi. Tipi di attacco. Crittoanalisi di cifrari affini, a sostituzione, di Vigenère, di Hill.

- Cenni di teoria di Shannon. Segretezza perfetta. Caratterizzazione dei crittosistemi a segretezza perfetta. One-time pad. Cifrari a flusso. Registri a scorrimento lineari.

- Crittosistemi prodotto. Reti a sostituzione-permutazione. Cifrari di Feistel. Data Encryption Standard. Triplo DES. Advanced Encryption Standard (AES). Modalità di funzionamento.

- Introduzione alla crittografia a chiave pubblica. Cenni di teoria della complessità. Problema dello zaino. Cifrario di Merkle-Hellman.

- Il crittosistema RSA. L'algoritmo square and multiply. Test di primalità. RSA e fattorizzazione. Alcuni attacchi all'RSA. Cenni sul cifrario di Rabin.

- Il problema del logaritmo discreto. Scambio della chiave di Diffie-Hellman. Il crittosistema di Elgamal.

- Firma digitale. Schemi di firma. Lo schema RSA. Lo schema di Elgamal.

- Cenni su alcuni protocolli crittografici: secret splitting e secret sharing.

- Aritmetica modulare. Definizione di gruppo. Gruppi ciclici. Permutazioni. Congruenze, funzione di Eulero, elementi invertibili in $\mathbb{Z}_n$. Cenni sui campi finiti. Teorema di Eulero, piccolo teorema di Fermat. Cenni sull' algoritmo di Euclide per il calcolo del MCD.

- **Seminari svolti dagli studenti:** Due finalisti dell'AES: Serpent e Twofish. Generatori di numeri pseudocasuali. Dal WEP al WPA. La crittografia durante la seconda guerra mondiale. Side channel attacks.