

**Programma del corso di Crittografia 1**  
**per l'a.a. 2017/18**  
**II semestre**  
**(Francesca Merola)**

- Introduzione alla crittografia. Cenni storici. Definizione di crittosistema. Cifrari classici. Introduzione alla crittoanalisi.
- Introduzione alla crittografia a chiave pubblica. Cenni di teoria della complessità. Algoritmi polinomiali e esponenziali. Problema dello zaino. Cifrario di Merkle-Hellman.
- Il crittosistema RSA. Test di primalità, Test di Solovay-Strassen. Test di Miller-Rabin. Algoritmi di fattorizzazione,  $p-1$  di Pollard, Rho di Pollard, Dixon's Random Squares. Alcuni attacchi all'RSA. Cifrario di Rabin.
- Il problema del logaritmo discreto. Scambio della chiave di Diffie-Hellman. Il crittosistema di Elgamal. Algoritmo di Shanks. Algoritmo di Pohlig-Hellman. Index Calculus.
- Doppio lucchetto/three-pass protocol: il crittosistema di Massey-Omura. Firma digitale. Schemi di firma. Lo schema RSA. Lo schema di Elgamal. Cenni su alcuni protocolli crittografici.