Programma provvisorio del corso di Crittografia 1
per l'a.a. 20016/17
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. Problema dello zaino. Cifrario di Merkle-Hellman.
- Il crittosistema RSA. Test di primalità. Algoritmi di fattorizzazione. Alcuni attacchi all'RSA. 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.