Estratto crittografia RSA

- Scegliere **due numeri primi** **p e q**
- Calcolare **n = pq**
- Mediante la **f = φ(n) di Eulero** posso sapere quanti sono i numeri compresi tra 1 e n che siano coprimi con n e ne scelgo uno che chiamo **e**
- Calcolare l'**inverso (mod f)** di **e** che identifico con **d**
- La coppia **(n, e)** *è la* ***chiave pubblica***
- La coppia **(n, d)** *è la* ***chiave privata***
- Non è possibile risalire facilmente dalla chiave pubblica a quella privata (e viceversa), in quanto servirebbe conoscere il numero (p-1)(q-1), e questo implica fattorizzare n nei suoi fattori p e q (problema difficile)