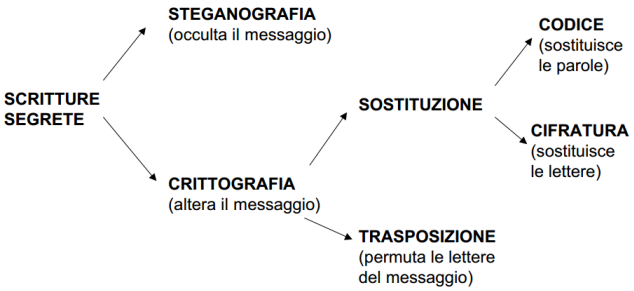
Crittografia e Aritmetica Modulare

I incontro

- Presentazione e definizioni
    - steganografia (inchiostro simpatico, microdot…)
    - crittografia-crittoanalisi (trasposizione, sostituzione)

Che cos'è la crittografia



- Distinzione fra cifrare/decifrare e codificare/decodificare
- Utilizzo: tradizionale (militare: guerre, complotti) e moderno (comunicazioni in rete, acquisti online)
- Crittografia nella storia:
    - Antichità (scitale, Erodoto)
    - Cifratura di Cesare
    - Rinascimento: Leon Battista Alberti e Blaise de Vigenere
    - Sostituzione monoalfabetica e polialfabetica
    - Babbage
    - Sviluppo macchine: dai dischi rotanti alla macchina Enigma
- Passaggio dalla chiave unica alla chiave pubblica
- Matematica e crittografia
- Esercizi – laboratorio

II incontro

- Il mondo dei numeri interi
    - la fattorizzazione unica
    - la divisione intera
    - il massimo comune divisore
    - l'algoritmo di Euclide e la formula di Bezout
- Esercizi – laboratorio
- L'aritmetica modulare
    - le classi resto modulo *n*
    - le operazioni di addizione e moltiplicazione in $\mathbf{Z}_n$
    - elementi invertibili in $\mathbf{Z}_n$ e determinazione dei loro inversi
- Esercizi – laboratorio

III incontro

- La funzione di Eulero
    - Definizione
    - proprietà moltiplicativa su fattori coprimi
    - calcolo effettivo
- Approfondimento: prodotto diretto di classi resto e Teorema Cinese del Resto.
- Esercizi – laboratorio

IV incontro

- I teoremi di Eulero e Fermat
    - le potenze in $\mathbf{Z}_n$
    - il Piccolo Teorema di Fermat
    - il Teorema di Eulero-Fermat
- la sorprendente applicazione al sistema crittografico RSA
- un primo semplice esempio
- Esercizi – laboratorio

V incontro

- Il Metodo crittografico RSA (Rivest, Shamir, Adleman)
    - la scrittura *m*-aria di un numero intero
    - codifica/decodifica di pacchetti di testo nell'alfabeto con *m* caratteri come elementi di $\mathbf{Z}_n$
    - l'algoritmo di codifica e decodifica effettivo
- Perché RSA è un sistema crittografico sicuro?
- Esercizi – laboratorio

VI incontro

- Autenticazione in crittografia RSA
    - la firma digitale
    - la certificazione delle chiavi crittografiche
    - la marcatura temporale
- Esercizi – laboratorio

VII incontro

- Test di fine corso