

1. Un modo per condividere segreti in maniera sicura

Supponiamo che un numeroso gruppo di scienziati sia al lavoro su un progetto segretissimo. I documenti del progetto vengono tenuti segreti in una cassaforte dove la combinazione segreta è sconosciuta a ciascun membro del gruppo. Vogliamo però che la cassaforte possa essere aperta se almeno sei membri del gruppo di ricerca sono presenti ma che la combinazione rimanga segreta se ci sono meno di 6 membri presenti.

Supponiamo che la combinazione sia un numero che chiamiamo a_0 . Costruiamo un polinomio $p(x)$ di grado 5 che abbia termine noto uguale ad a_0 , e dei numeri arbitrari (fissati) per i restanti coefficienti

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$$

Distribuiamo a ciascuno dei membri del gruppo di ricerca un valore $p(x_i)$ (con $x_i \neq 0$). Non appena 6 membri si riuniscono essi possono calcolare i polinomi di Lagrange relativi ai punti $\{x_{i_0}, x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}, x_{i_5}\}$ e ottenere

$$\begin{aligned} p(x) = & p(x_{i_0})\delta_0(x) + p(x_{i_1})\delta_1(x) + p(x_{i_2})\delta_2(x) \\ & + p(x_{i_3})\delta_3(x) + p(x_{i_4})\delta_4(x) + p(x_{i_5})\delta_5(x) \end{aligned} \quad (1.1)$$

Dopodiché non devono far altro che leggere il termine noto del polinomio così determinato.

Esercizio. Determinare la combinazione segreta determinata dai valori distribuiti a lezione.