Secret sharing – om at dele en hemmelighed
Johan P. Hansen

Secret sharing henviser til metoder til fordeling af en hemmelighed blandt en gruppe af deltagere, som hver især får tildelt en andel (en share) af hemmeligheden.

Hemmeligheden kan rekonstrueres, når et tilstrækkeligt antal af andele (shares) er kombineret sammen, hvorimod få andele (shares) ikke er til nogen nytte.

Hemmelighed deles ved at hver af de *n* spillere får en andel (share) på en sådan måde, at enhver mængde af *t* (for tærskel) eller flere spillere sammen kan rekonstruere hemmeligheden, men ingen gruppe af færre end t spillere kan. Et sådant system kaldes en (*t, n*) – tærskel system.

Secret deling blev opfundet uafhængigt af Adi Shamir og George Blakley i 1979.

Vi vil beskæftige os med Shamirs system, der matematisk bygger på evaluation og interpolation af polynomier, og ville kunne behandles umiddelbart i gymnasieskolen.