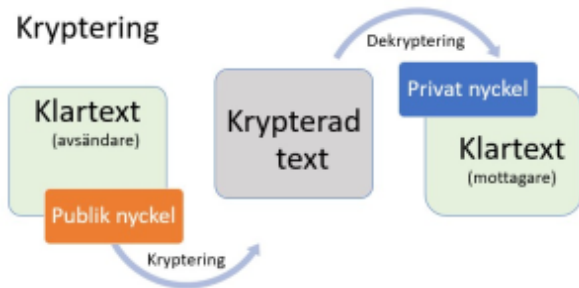


PGP

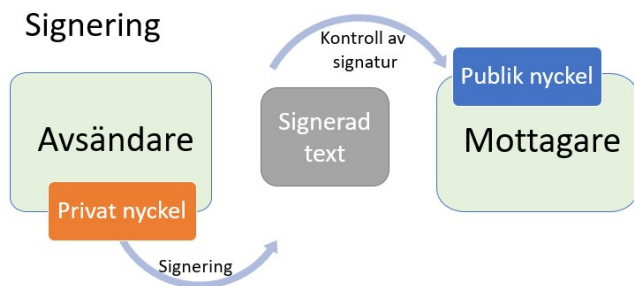
PGP (Pretty Good Privacy) är en defacto-standard för att signera och kryptera data. PGP används både för att skicka signerad/krypterad mail eller för att signera/kryptera fristående filer.

PGP använder sig av asymeterisk kryptering, dvs du har en egen privat nyckel som bara du känner till. Sedan har du en publik nyckel som du kan dela med alla som vill kontrollera din signatur eller skicka krypterad data till dig.

Kryptering: Du har en text/mail som du vill kryptera så att endast mottagaren kan läsa det. Du krypterar med mottagarens publika nyckel. Mottagaren dekrypterar det sedan med sin privata nyckel.



Signering: Du har en text som du vill vara säker på går att kontrollera att det är just du som skickat den. Du signerar med din privata nyckel. Mottagaren kontrollerar sedan signaturen med din publika nyckel.



Det går bra att både signera och kryptera en och samma fil/mail.

Diskussioner, anvisningar etc finns på SUNET Forum: <https://forum.sunet.se> - "PGP - Nyckelförmedling"