

Kryptering



Introduksjon

I dette dokumentet gis en basis forklaring på en teknikk brukt til kryptering av dokumenter og hvordan man skal kunne installere nødvendig programvare og gå gjennom de stegene som behøves for å få kryptert filen.

I denne løsningen gjør vi bruk av den åpne standarden OpenPGP.

Vi tatt utgangspunkt i programmet GPG4Win versjon 1.1.3. som er en sammenstilling av flere verktøy innen kategorien. Programmet kan kjøres på Windows (2000/XP/2003/Vista). Programmet er testet på "Windows XP" og "Windows Vista Home Premium"

Denne installasjonsveiledningen beskriver installasjon på Windows XP.

Asymmetrisk kryptering

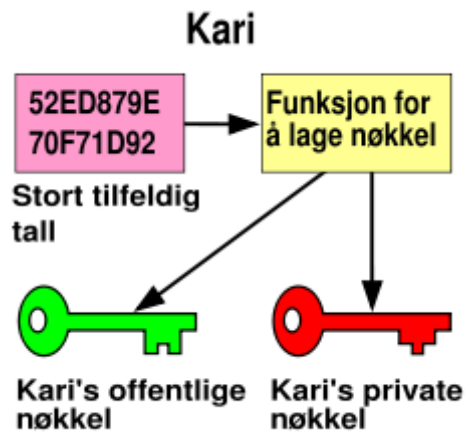
Dette avsnittet er hentet fra Wikipedia, den frie encyklopedi

Asymmetrisk kryptering, også kjent som **offentlig nøkkelkryptering**, er en form for kryptering hvor en bruker har et par med kryptografiske nøkler - en offentlig nøkkel og en **privat nøkkel**. Den private nøkkelen holdes hemmelig, mens den offentlige nøkkelen kan gis ut til hvem som helst. Nøklene er matematisk relaterte, men den private nøkkelen kan ikke avledes fra den offentlige nøkkelen på en praktisk måte. En melding kryptert med den offentlige nøkkelen kan kun dekrypteres med den tilsvarende private nøkkelen.

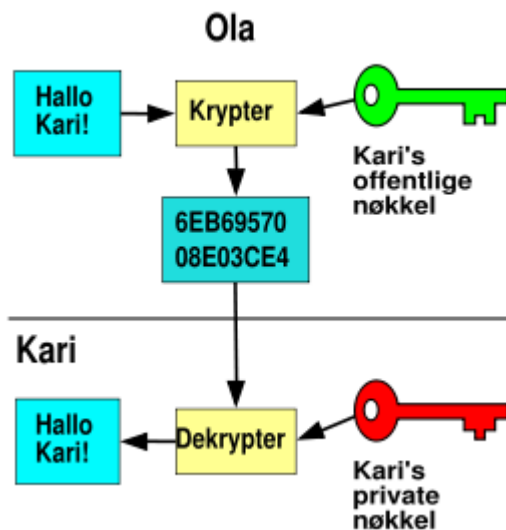
Til sammenligning, benytter symmetrisk kryptering en enkel privat nøkkel for både kryptering og dekryptering.

De to hovedgrenene av asymmetrisk kryptering er:

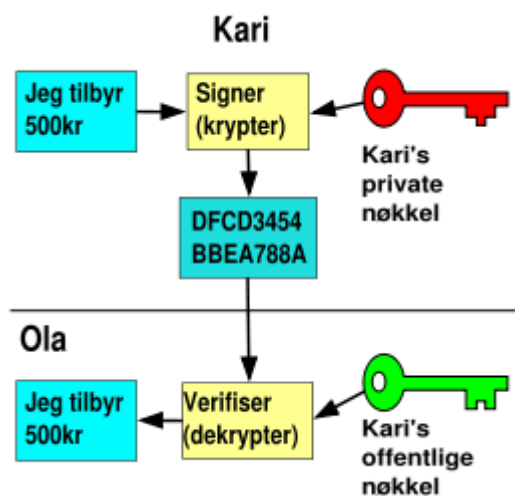
- **Offentlig nøkkelkryptering** – en melding kryptert med en brukers offentlige nøkkel kan ikke dekrypteres av andre enn brukeren som har den tilsvarende private nøkkelen. Dette brukes for å sikre fortroligheten.
- **Digitale signaturer** – en melding signert med en brukers private nøkkel kan verifiseres av hvem som helst som har tilgang til brukers offentlige nøkkel, og dermed bevise at brukeren har signert den samt at meldingen ikke har blitt endret. Dette benyttes for å godtgjøre ekteheten.



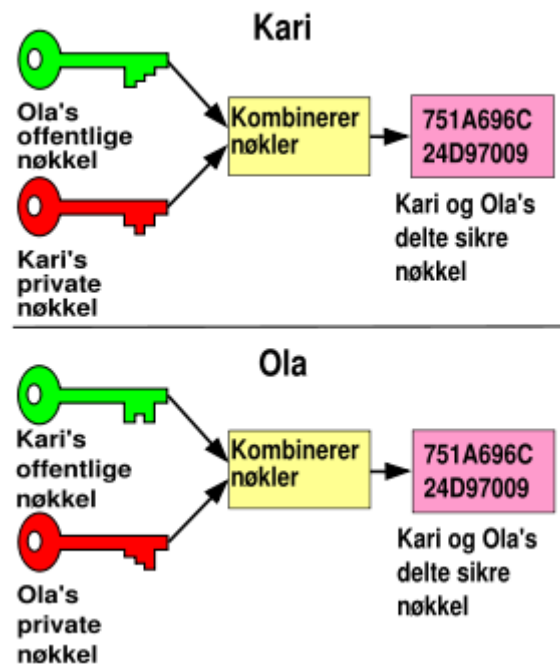
Et stort tilfeldig tall blir brukt til å lage et offentlig nøkkelpar.



Hvem som helst kan kryptere med den offentlige nøkkelen, men kun innehaveren av den private nøkkelen kan dekryptere. Sikkerheten avhenger av sikkerheten til den private nøkkelen.



Ved å benytte en privat nøkkel til å kryptere (dvs. signere) en melding, kan alle verifisere denne signaturen med den offentlige nøkkelen. Verifiserbarhet avhenger av sikkerheten til den private nøkkelen.



Ved å kombinere din egen private nøkkel med andres offentlige nøkler, kan man regne ut en delt sikker nøkkel som bare dere vet. Den delte sikre nøkkelen kan brukes som nøkkelen til en symmetrisk krypteringsalgoritme.

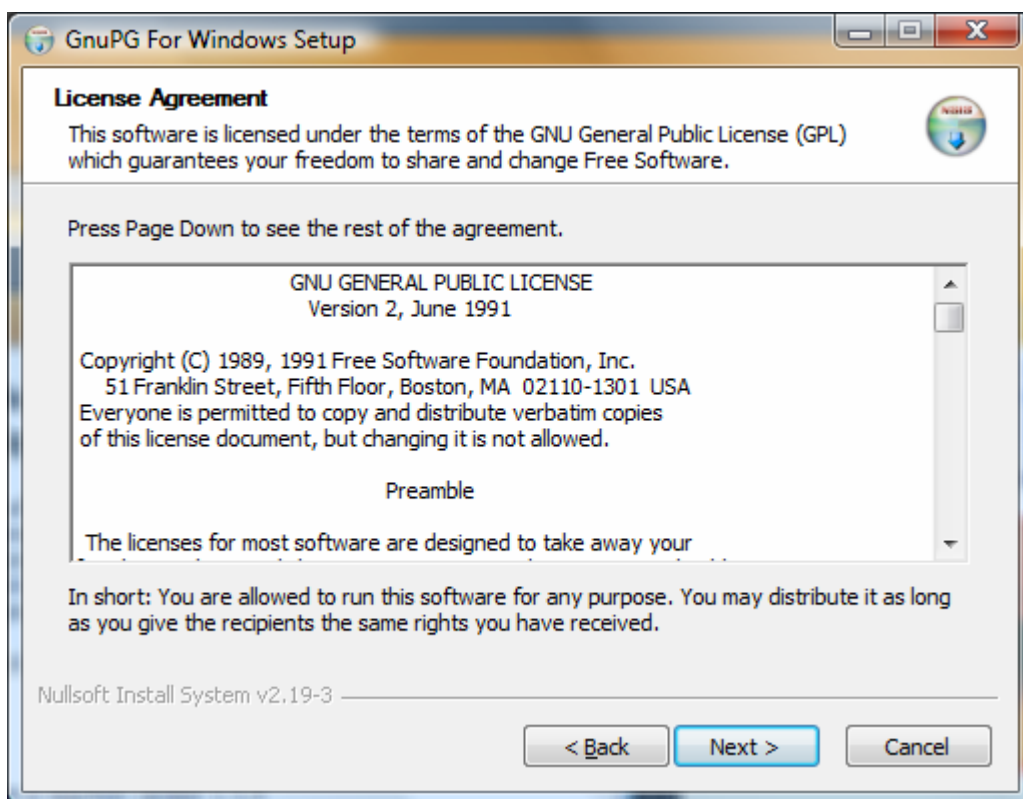
Programvare

Det finnes flere programmer som kan anvendes til et krypteringsformål. Her har vi tatt utgangspunkt i programmet GPG4Win versjon 1.1.3. som er en sammenstilling av flere verktøy innen kategorien. Programmet kan kjøres på Windows (2000/XP/2003/Vista).

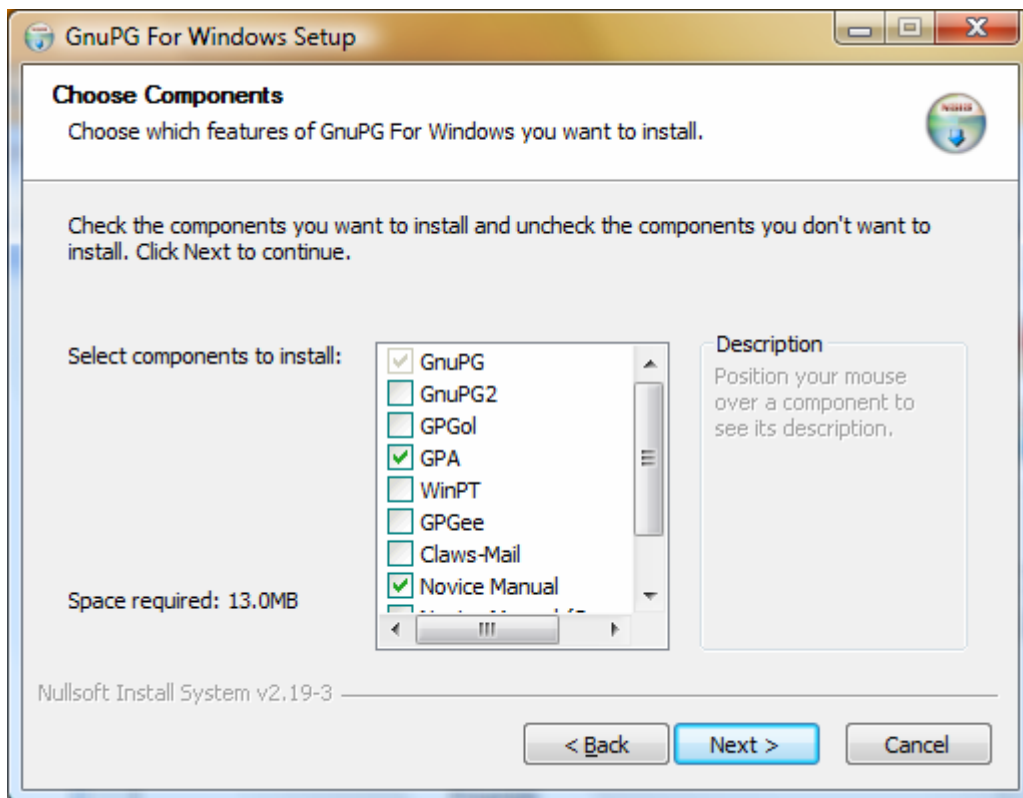
Installasjon



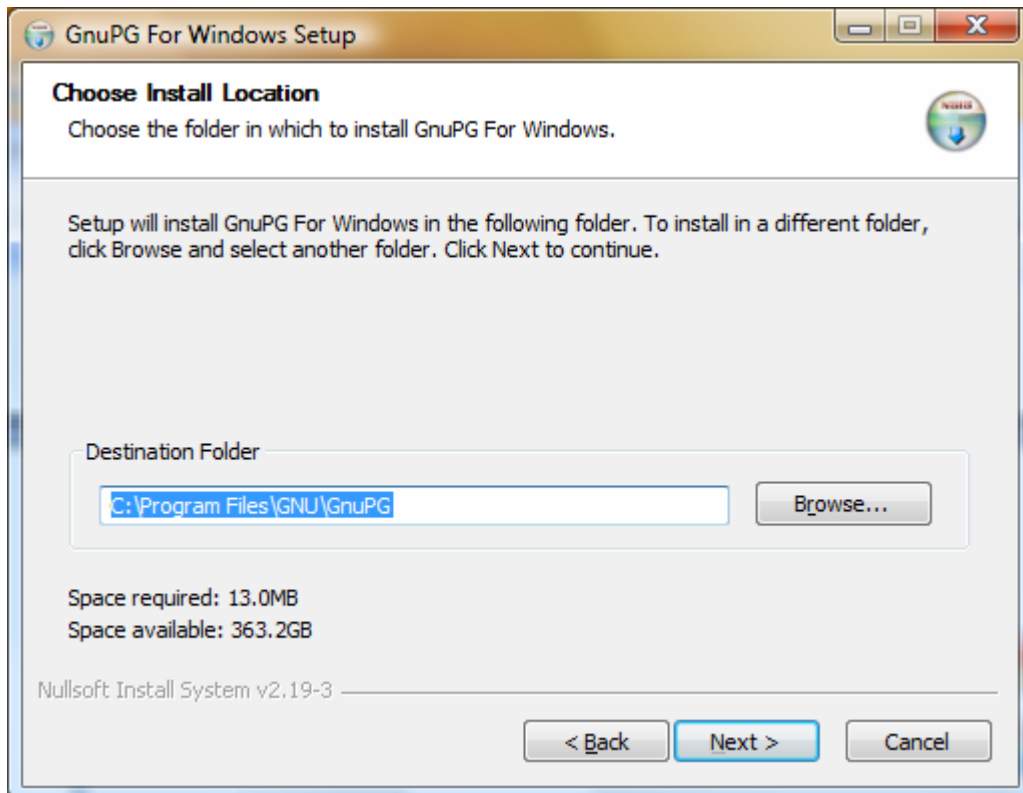
Trykk Next



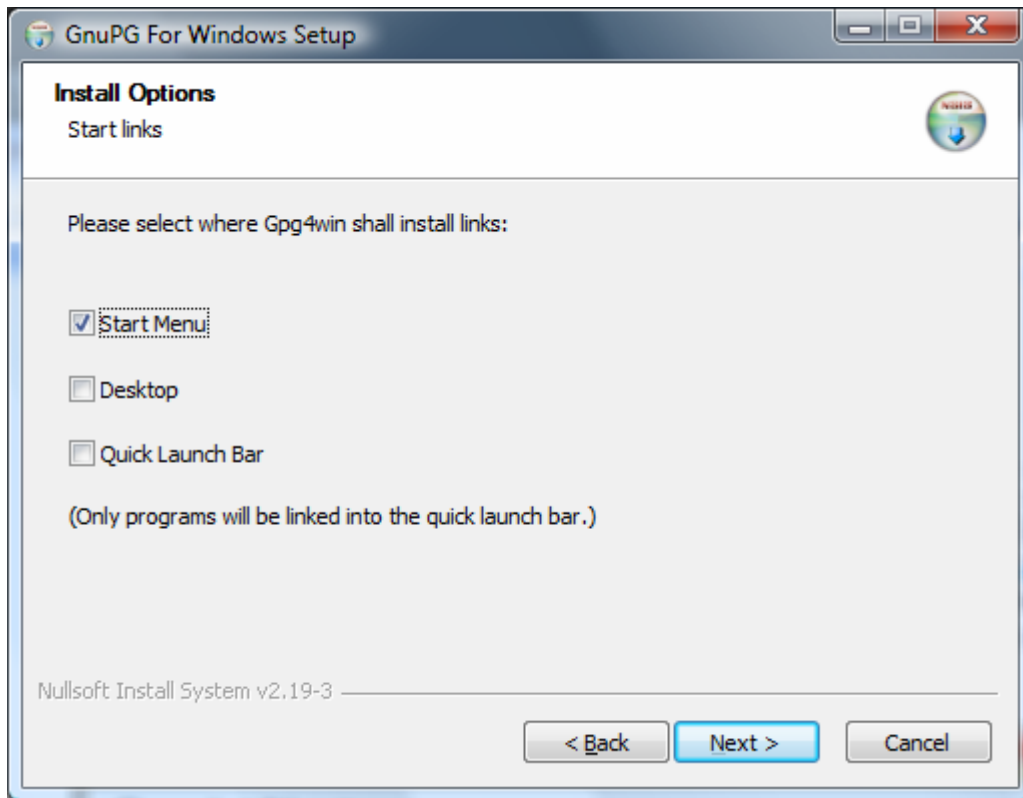
Trykk Next



I dette skjermbildet velger man hvilke komponenter man ønsker å installere. Man kan velge de verktøyene man ønsker, men velg minimum 'GPA' som angitt ovenfor. Foruten GnuPG kan alt annet velges bort om man ønsker. Trykk så Next



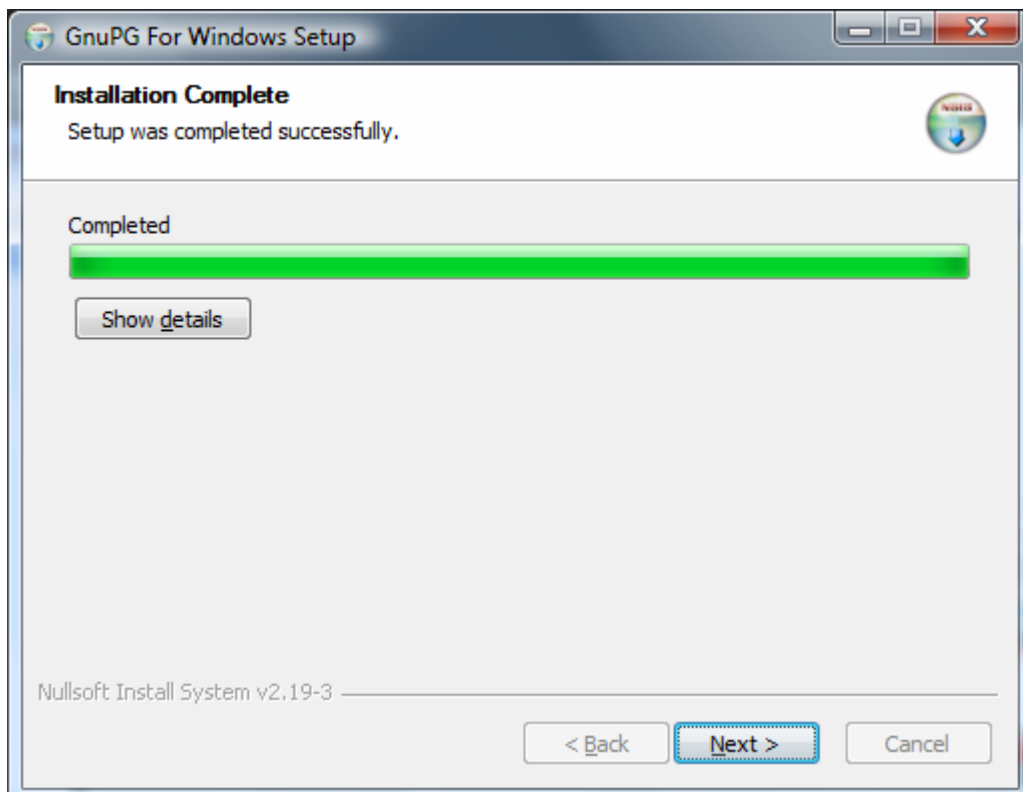
Trykk Next



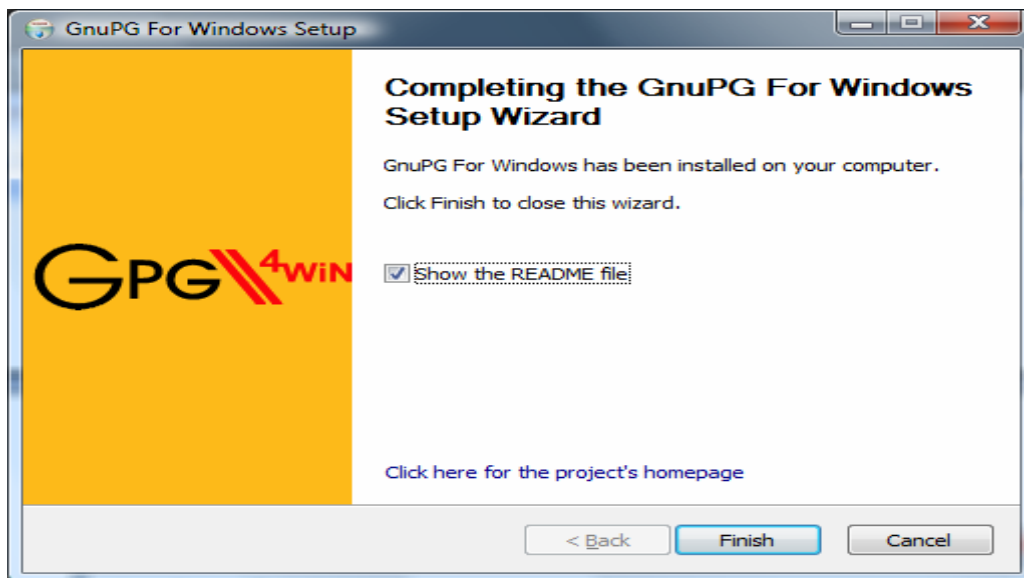
Velg plassering av ikonet som brukes for starte programmet. Velg 'Start Menu' og eventuelt 'Desktop' dersom det gjør det lettere å finne det.

s

Trykk Install



Når installasjonen er ferdig skal man ha en dialogboks som den ovenfor. Velg da 'Next'



Velg 'Finish'

README filen som kommer opp kan man lese gjennom og deretter lukke.

Du har da opprettet en mappe i startmenyen som heter 'GnuGP for Windows'. I denne finner du programmet GPA (Gnu Privacy Assistant) som vi skal bruke.