Krypteringskurs

og nøkkelsigneringsfest.

Fredag 2021-11-19 kl. 17.15

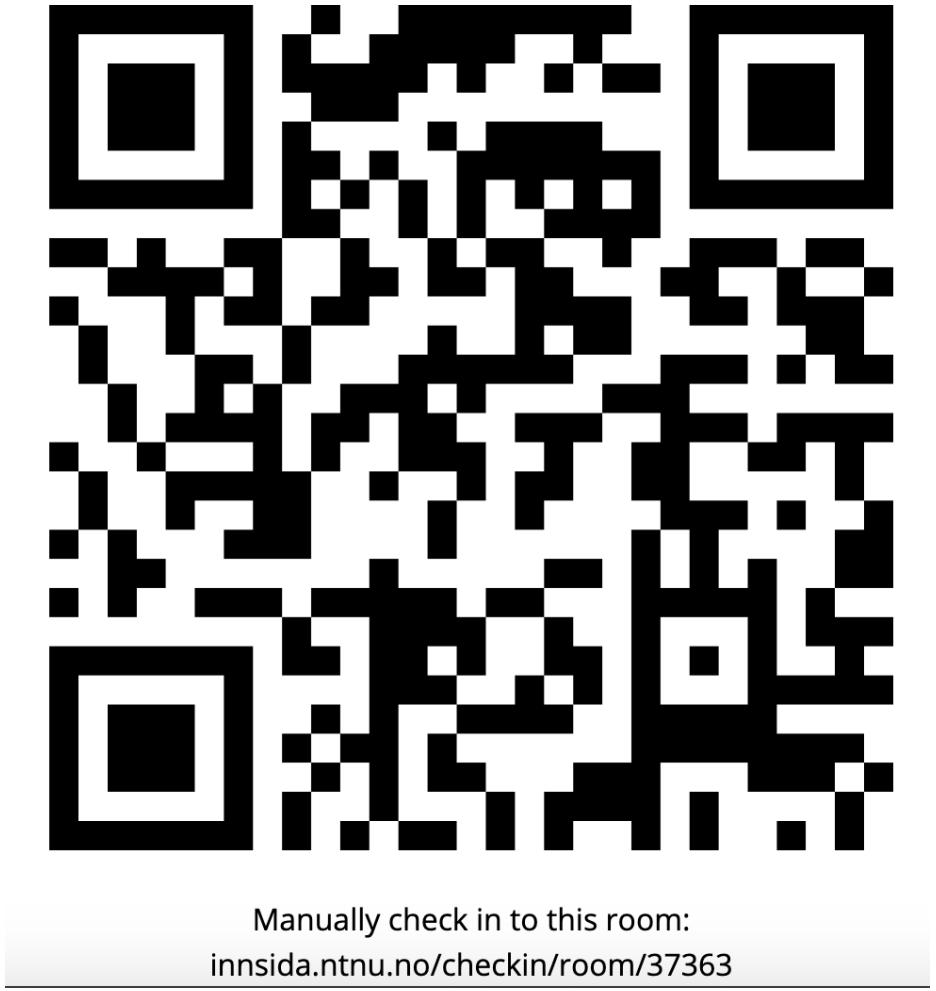
Arrangert av NVG og PVV

Gunnar René Øie

David Kaasen

Smittevern

- Husk smittevern-rådene
- Vennligst sjekk inn i rommet:
  - QR-kode, eller
  - innsida.ntnu.no/checkin/room/37363



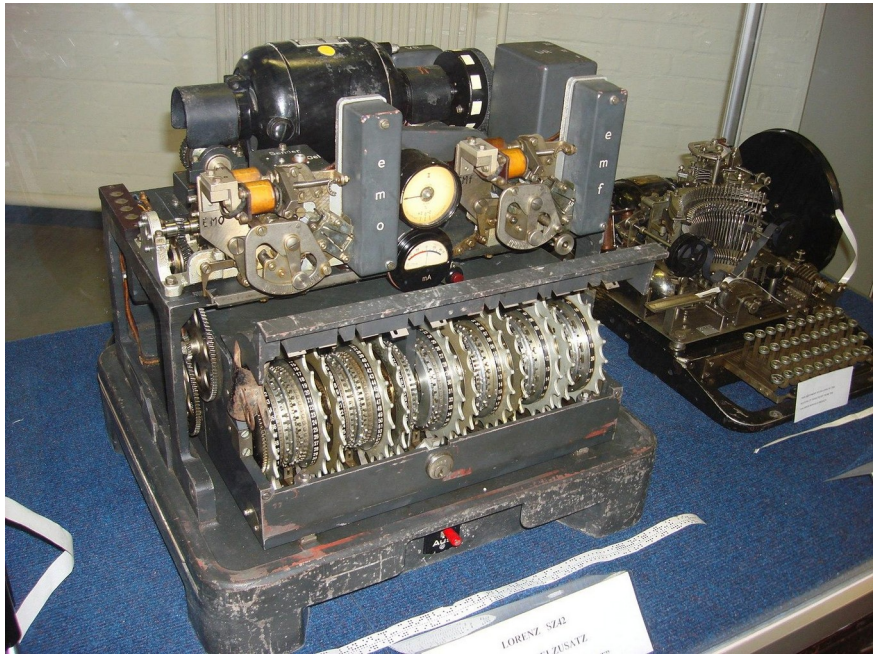
Del I. Kort intro til kryptografi.

- Sende hemmelige meldinger til noen.

og/eller

- Bekrefte at meldingen ikke har blitt tuklet med.

- Hemmeligheten har en viss holdbarhet.



Lorenz-maskin (foto: Garrethe, Public Domain)

Symmetriske nøkler.

- Tradisjonell kryptering.
- Eks. på kode:
- «foobar» --> «6-15-15-2-1-18»
- Nøkkelen må utveksles på en fortrolig måte.

Klartekst	Krypto-tekst
a	1
b	2
c	3
...	...
å	29

Dette er en nøkkel.

Asymmetriske nøkler.

- Forholdsvis nytt (1970-tallet).
- Offentlig nøkkel + privat nøkkel.
- Lett å utveksle.
- Kan brukes til signering.
- Problem: Er nøkkelen autentisk?
- Mulig løsning: Tillitsvev.

Del II. Hvordan bruke GnuPG.

- GnuPG («GNU Privacy Guard») er en FOSS-implementasjon av OpenPGP-standarden.
- PGP («Pretty Good Privacy») er en annen, proprietær implementasjon.
- Hovedprogrammet i GnuPG heter `gpg`.
  - Også enklere programmer som `gpgv` (verifisering av filer)
- Hjelp kan fås med kommandoen `man gpg`

Begreper.

- «Nøkkel» er tvetydig.
  - Én enkelt, offentlig eller privat nøkkel.
  - Et slikt nøkkelpar.
- To typer signering:
  - Signere nøkler, også kalt sertifisering.
  - Signere meldinger.
- Kapabiliteter:
  - C: nøkkelsignering
  - S: meldingssignering
  - E: kryptering
  - A: autentisering

- Hoved- og undernøkler.
  - Hovednøkkelen signerer andre nøkler, inkl. undernøklene. Bare hovednøkkelen kan ha kapabilitet C.
  - Undernøkler kan ha resten av kapabilitetene, typisk én hver. Kan opprettes og tilbakekalles ila. levetiden til hovednøkkelen, som man vil.
- All nøkkelinformasjon ligger under `~/.gnupg`
- Nøkler og nøkkelsignaturer ligger i en nøkkelring.
- Identitet. Navn, e-postadresse, portrettbilde o.l.

- Nøkkel-id. Identifiserer hovednøkkelen. F.eks. 4EF63FCBDBE10804C1EF07721FCEC24586B458D5.
  - Ofte brukes de siste 8 tegnene: f.eks. 86B458D5
- Nøkkelfingeravtrykk. Samme som id-en, men delt opp i segmenter.

Hvordan bruke GnuPG

- Kommandolinje (Linux, BSD, MacOS og Windows)
- Linux GUI: GPA, KGpg, Kleopatra eller Seahorse
- MacOS GUI: GPG Suite https://gpgtools.org/
  - Gratis GUI-versjon av GPG
  - Nøkkelhåndtering
  - Kryptering/dekryptering av tekst i alle programmer via merking og meny
  - Tettere integrasjon med Mac Mail koster penger; dekrypter uten ekstra klikk
- Windows GUI: https://gpg4win.org/
  - Nøkkelhåndterer (Kleopatra)
  - Integrasjon med Outlook
  - Andre verktøy for signering av filer osv.

GnuPG i praksis.

Kryptering:

```
$ cat melding
Hallo, verden!
$ gpg --armour --encrypt --recipient alice@example.net melding
$ cat melding.asc
-----BEGIN PGP MESSAGE-----

hQIMAzqs+6klAb1FARAAnKuxKBlZl2aG3/MANuatekHcnPyPqtwhxt9TaJ+LolfJ
lxU7EnEsS0K/3bFZdBEZo1Umf5Qaz0dR+Jp3r0yWS/VZjblMk9bP2IjhX0csTcK4
[…]
UQEUYzyI86+5rtUC3vrjAJSlzJQd6CiaAiw9O7WGtrTbIgjK1Hycv5cAodsQgfVT
m4osyJ6uvUMXUHIwPNKFBopafMfJ6XWjah6bucWysE0TYQ==
=vMz3
-----END PGP MESSAGE-----
```

•

Dekryptering:

$ gpg --decrypt -o - melding.asc

gpg: encrypted with 4096-bit RSA key, ID 3AACFBA92501BD45, created 2012-09-15

"David Kaasen <kaasen@nvg.ntnu.no>"

Hallo, verden!

Meldingssignering.

```
$ gpg --clear-sign melding
$ cat melding.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Hallo, verden!
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEEfEoJEeXz8rSNjeAYrM6iUplrDcFAl+E5UIACgkQYrM6iUpl
rDf2JBAAu+8bUKUdMJkQr38hY50zDoQ3914BMHSgZhEUW40v8LOEucT73bTyM907
[…]
+UKKXylMhtHQ0Tej4XX1879+lYfI3lXCgLI0DepcySA/6ooI83Y=
=s+x5
-----END PGP SIGNATURE-----
```

Verifisering.

```
$ gpg --verify melding.asc
gpg: Signature made ti. 13. okt. 2020 kl. 01.22 +0200 CEST
gpg:                using RSA key 11F128244797CFCAD236378062B33A894A65AC37
gpg: Good signature from "David Kaasen <kaasen@nvg.ntnu.no>" [ultimate]
gpg:                 aka "David Kaasen <davidk@pvv.org>" [ultimate]
gpg:                 aka "David Kaasen <kaasen@nvg.org>" [ultimate]
gpg:                 aka "David Kaasen <davidk@pvv.ntnu.no>" [ultimate]
```

Opprette nøkler.

```
$ gpg --full-gen
```

Legg til flere identiteter eller undernøkler:

```
$ gpg --edit-key --expert <nøkkel-id>
gpg> addkey
gpg> adduid
gpg> save
```

Nøkkelsikkerhet.

- Viktig med god passfrase.
- Tilbakekallingssertifikat: Lag det når du oppretter nøkkelen.
- Sikkerhetskopi.
- Privat hovednøkkel kun på offline-maskin eller live-USB-pinne.
  - Kopier nøklene.
  - Slett den private nøkkelen fra dagligmaskinen.
  - Bruk undernøkler til daglig

```
$ gpg --delete-secret-keys <nøkkel-id>
# Svar «nei» for subnøkler.
```

Signering utenfor selve datamaskinen

- Mulig å gjøre signeringen utenfor selve datamaskinen
- Spesielle smartkort og USB-enheter som holder privatnøkkelen uten at datamaskinen får tilgang til den den, men får bruke den til signering når man fysisk trykker på enheten
- Privatnøkkel kan
  - opprettes på enheten (mest sikkert)
  - importeres fra datamaskinen
- En Yubikey kan brukes til my annet enn GPG
  - Innlogging på Facebook, Google osv.
  - Innlogging på PC osv.

Yubikey

Nøkkelutveksling

- Hvordan utveksle offentlige nøkler direkte
- Hvordan utveklse offentlige nøkler via tjenere
  - Sertifikat-utstedere
  - Tillitsvev "Web of trust" - stoler du på at dine venner kjenner sine venner?

Laste offentlige nøkler opp og ned.

Bruk en web-of-trust-nøkkeltjener:

```
$ echo keyserver pgp.mit.edu >> ~/.gnupg/gpg.conf
$ echo keyserver-options no-self-sigs-only >> ~/.gnupg/gpg.conf
```

Last opp:

```
$ gpg --send-keys <nøkkel-id>
```

Last ned:

```
$ gpg --search-keys <søketekst>
```

Eller hvis du har nøkkel-id-en:

```
$ gpg --recv-keys <nøkkel-id>
```

Alternativ til å bruke nøkkeltjener

- Send den offentlige nøkkelen som vedlegg til eposter
  - Slipper at spam-roboter snapper opp epost-adressen din
  - Vanskeligere for andre å finne nøkkelen din
  - Verken mer eller mindre sikkert enn å utveksle nøkkel via sentral server – det viktige er om du stoler på de som har signert bruker-ID'ene
- Ferdig installerte sertifikatkjeder
  - Nettlesere og operativsystemer kommer med rot-sertifikater som de stoler på.
  - Utstederes ansvar å sjekke hvem de utsteder sertifikater til etter en sertifikat-politikk (policy)
  - Det har skjedd at utstedere ved feil og/eller med vilje har utstedt sertifikater til folk som ikke burde fått dem

Signere andres nøkler (1/2)

Finurlighet ved å gå god for en nøkkel basert på legitimasjon:

- Selv om du vet at personen mest sannsynlig heter det navnet, hvordan vet du at personen eier den epost-adressen?
  - Bill Gates (1955-10-28)
  - bill@microsoft.com
  - bill@ntnu.no

Samme person?

- Du signerer egentlig på hver bruker-ID som er tilknyttet nøkkelen.
- Alternativ Bruker-ID: Navn + Fødselsdato uten epost
- Signer kun bruker-ID'er som du går god for at vedkommende eier

Signere andres nøkler (2/2)

- Signer én identitet om gangen, send på e-post, slett nøkkel, last ned på ny og gjenta med neste identitet.

```
$ gpg --sign-key <nøkkel-id>
# Eventuelt:
gpg> uid 1
gpg> sign
gpg> save
# Krypter og signer meldingen.
$ gpg --armor --export someone@example.com > ~/someone_at_example.com.asc
$ gpg --armor --sign --encrypt --recipient someone@example.com \
   ~/someone_at_example.com.asc
```

Motta signert nøkkel.

```
$ gpg --decrypt someone_at_example.com.asc.pgp | gpg –import
# Last opp nøkkelen din.
```

Hvor mye stoler du på andres signeringer?

```
$ gpg --edit-key <nøkkel-id>    eller
$ gpg --edit-key <epost-adresse>

pub  rsa4096/D4B4EE41D24107CF
(....)
gpg> trust
(....)
Velg hvor mye du stoler på at denne brukeren kan bekrefte
andre brukeres nøkler (ved å se på pass, sjekke fingeravtrykk fra
forskjellige kilder, osv.)

  1 = Jeg vet ikke eller vil ikke uttale meg
  2 = Jeg stoler IKKE på den
  3 = Jeg stoler marginalt
  4 = Jeg stoler fullt
  5 = Jeg stoler fullstendig på den
  m = tilbake til hovedmenyen

Hva velger du?
```

Symmetrisk kryptering.

`gpg` kan også brukes til symmetrisk kryptering. Den eneste nøkkelen som da blir involvert, er den passfrasen man angir.

```
$ cat melding
Hallo, verden!
$ gpg --armour --symmetric melding
$ cat melding.asc
-----BEGIN PGP MESSAGE-----

jA0ECQMC6vHvoQkA9oD/0ksB7YO2XZF/0wVpKfIuUWF21wYrhMDSXnA19SelYLOx
cevQrsrNB3zchljwrcsgn/mRklTMmwmkfSzH3CLhy36RKVJXhrxaor+zUgw=
=xZrb
-----END PGP MESSAGE-----
```

Dekryptering er som for den asymmetriske varianten, men nøkkelen er den samme passfrasen som isted.

Del III. Generering og signeringsfest.

1. Vi genererer nøkler.
2. Last opp din egen offentlige nøkkel; evt. send den via epost til de som skal signere.
3. Hva er fingeravtrykket ditt?
4. Last ned andres nøkkel, signer når du har sjekket deres fingeravtrykk.
5. Send andres nøkkel tilbake til dem med din nøkkel-signatur, gjerne kryptert.

Nett: AndroidAP, passord: gpgkurset

Uten at fingeravtrykk utveksles på en sikker måte kan du ikke stole på nøklene.

Vanligvis anbefales det at signeringsfester utføres på papir, uten at noen har med datamaskinen sin.