NTNU

Norges teknisk-naturvitenskapelige universitet

Hvorfor er eID (u)sikkert?

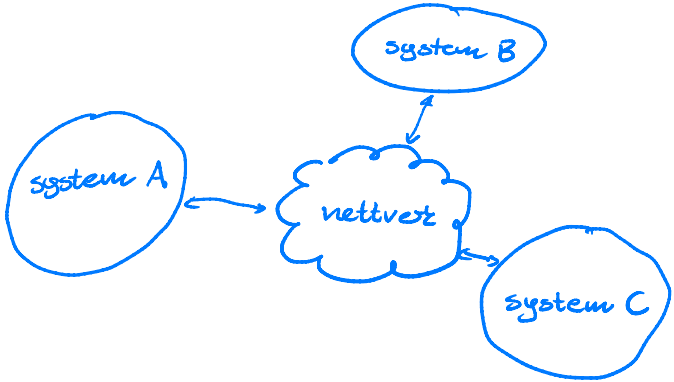
Kristian Gjøsteen
Institutt for matematiske fag
Bruk og misbruk av eID, 10. mars 2022

Hvem er jeg?

Professor i matematisk kryptologi.

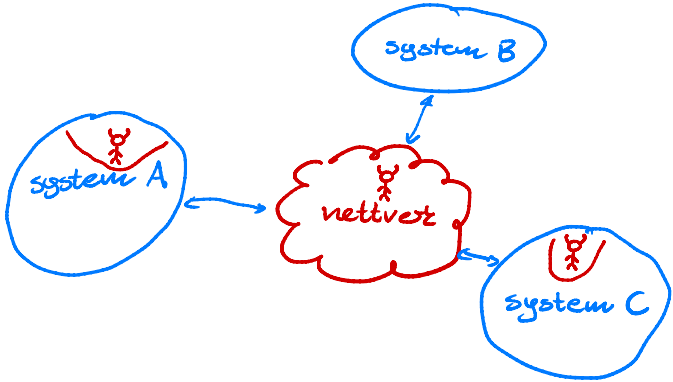
- Arbeider med å beskytte verden mot kvantedatamaskiner.
- Utdanner kryptologer (master/PhD).
- Med på SODI-prosjektet.
- Arbeidet med sikkerhet i eID.
- E-valg i Norge i 2011 og 2013.
- Medlem i Lysne-utvalget.

Hvordan ser kryptologer på verden?



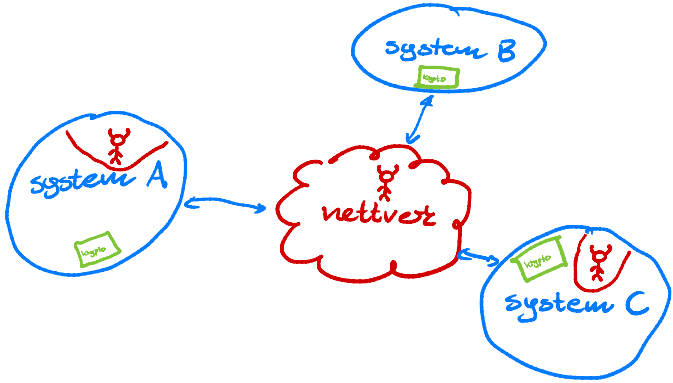
- En samling av systemer knyttet sammen av et nettverk.

Hvordan ser kryptologer på verden?



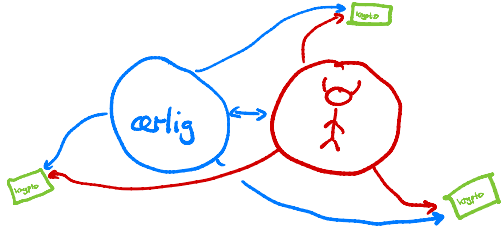
- Angriperen er nettverket. Og hele systemer. Eller deler av dem.

Hvordan ser kryptologer på verden?



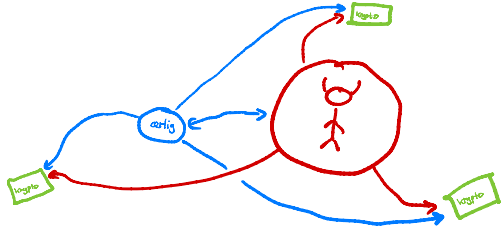
- Kryptografi finner vi noen få steder.

Hvordan ser kryptologer på verden?



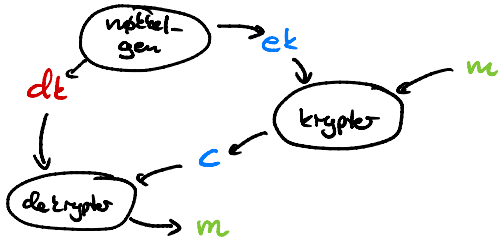
- Min verden består av (i) en angriper, (ii) noe jeg ikke vet hva er, og (iii) kryptografien min.
- Når jeg lager kryptografi vet jeg ikke hvordan den skal brukes.

Hvordan ser kryptologer på verden?



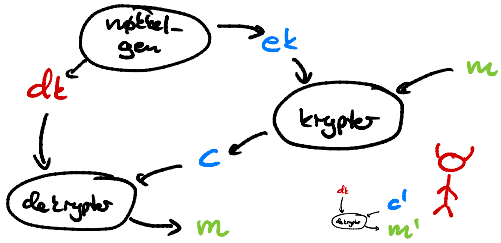
- Anta at systemet gjør sitt ytterste for å misbruke kryptografien min.
- Forenkler: Angriperen gjør det meste.

Hva er kryptering?



- Vi har krypteringsnøkler og dekrypteringsnøkler.
- Vi krypterer meldinger til chiffertekster med krypteringsnøkler.
- Vi dekrypterer chiffertekster til meldinger med dekrypteringsnøkler.
- OBS! Det er vanlig å kalle disse offentlige og private nøkler.

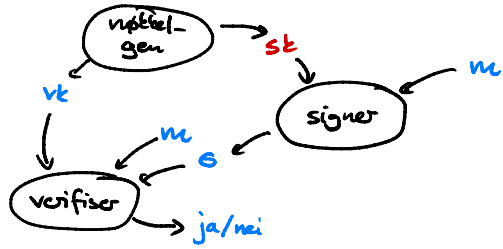
Hva betyr sikkerhet for kryptering?



Sikkerhet er at angriperen ikke får gjort det han vil.

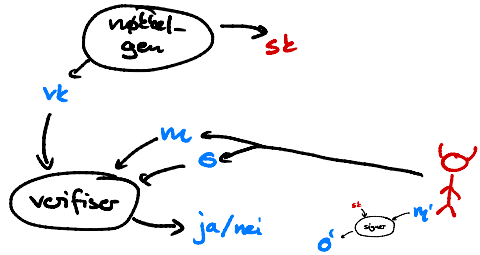
- Uten dekrypteringsnøkkelen vet du ingenting om dekrypteringene.

Hva er signaturer?



- Vi har signeringsnøkler og verifikasjonsnøkler.
- Vi lager signaturer på meldinger med signeringsnøkler.
- Vi verifiserer signaturer på meldinger med verifikasjonsnøkler.

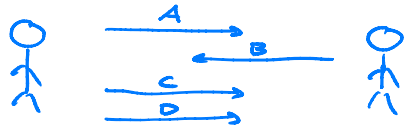
Hva betyr sikkerhet for signaturer?



Sikkerhet er at angriperen ikke får gjort det han vil.

- Uten signaturnøkkelen kan du ikke lage signaturer på nye meldinger.

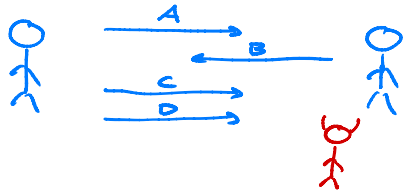
Samtaler



I en samtale snakker begge parter.

Sikkerhet er at angriperen ikke får gjort det han vil.

Samtaler

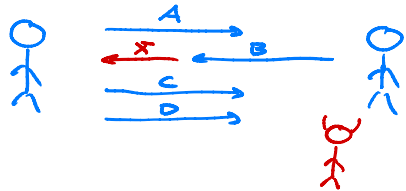


I en samtale snakker begge parter.

Sikkerhet er at angriperen ikke får gjort det han vil.

- Angriperen vil vite hva som sies.

Samtaler

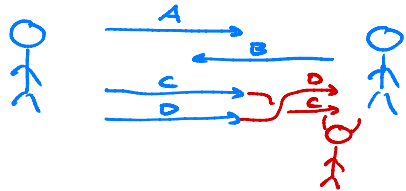


I en samtale snakker begge parter.

Sikkerhet er at angriperen ikke får gjort det han vil.

- Angriperen vil vite hva som sies.
- Angriperen vil forandre på det som høres.

Samtaler

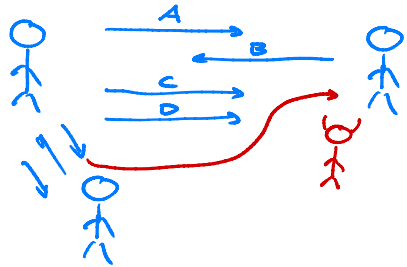


I en samtale snakker begge parter.

Sikkerhet er at angriperen ikke får gjort det han vil.

- Angriperen vil vite hva som sies.
- Angriperen vil forandre på det som høres.
- Angriperen vil forandre på samtalen.

Samtaler

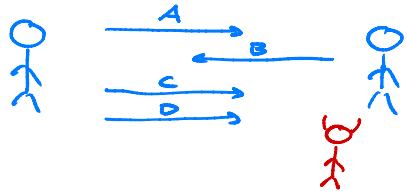


I en samtale snakker begge parter, med mange samtidige samtaler.

Sikkerhet er at angriperen ikke får gjort det han vil.

- Angriperen vil vite hva som sies.
- Angriperen vil forandre på det som høres.
- Angriperen vil forandre på samtalen.

Samtaler



I en samtale snakker begge parter, med mange samtidige samtaler.

Sikkerhet er at angriperen ikke får gjort det han vil.

- I en samtale er det bare partene som vet hva som ble sagt.
- I en samtale er begge parter enige om hva som er sagt, i hvilken rekkefølge. Og *hvilke nøkler som er i bruk*.

Hvor er menneskene?

Hva skiller Alice sine nøkler fra Eve sine nøkler?

- En *nøkkelinfrastruktur* lar Bob få tak i Alice sine nøkler.
- Infrastrukturen drives ofte av *tiltrodde tredjeparter*.

Hvor er menneskene?

Hva skiller Alice sine nøkler fra Eve sine nøkler?

- En *nøkkelinfrastruktur* lar Bob få tak i Alice sine nøkler.
- Infrastrukturen drives ofte av *tiltrodde tredjeparter*.
- Nøkkelinfrastrukturer kan ta mange former:
  - Hviskeleken?
  - Telefonkatalog?
  - Introduksjonsbrev?
  - Opplysningen?

Hvor er menneskene?

Hva skiller Alice sine nøkler fra Eve sine nøkler?

- En *nøkkelinfrastruktur* lar Bob få tak i Alice sine nøkler.
- Infrastrukturen drives ofte av *tiltrodde tredjeparter*.
- Nøkkelinfrastrukturer kan ta mange former:
  - Hviskeleken?
  - Telefonkatalog?
  - Introduksjonsbrev?
  - Opplysningen?
- OBS! Begrepet *«public key infrastructure»* har mange definisjoner.

Elektronisk signatur

En *elektronisk signatur* knytter et dokument til en person.

- Naivt: En digital signatur + en nøkkelinfrastruktur som kobler nøkler til personer.

Elektronisk signatur

En *elektronisk signatur* knytter et dokument til en person.

- Naivt: En digital signatur + en nøkkelinfrastruktur som kobler nøkler til personer.

Sikkerhet er at angriperen ikke får gjort det han vil.

- Alice' elektroniske signatur på et dokument er laget av Alice. Og Alice mente å lage den.

Elektronisk identifikasjon

Elektronisk identifikasjon er en samtale mellom personer, der begge vet hvem den andre er.

- Naivt: En samtale beskyttet med kryptografi + en nøkkelinfrastruktur som kobler nøkler til personer.

Elektronisk identifikasjon

Elektronisk identifikasjon er en samtale mellom personer, der begge vet hvem den andre er.

- Naivt: En samtale beskyttet med kryptografi + en nøkkelinfrastruktur som kobler nøkler til personer.

Sikkerhet er at angriperen ikke får gjort det han vil.

- Bare personene i samtalen vet hva som ble sagt.
- Begge parter er enige om hva som er sagt, i hvilken rekkefølge. Og *hvem det er sagt til*.

Elektronisk identifikasjon

Elektronisk identifikasjon er en samtale mellom personer, der begge vet hvem den andre er.

- Naivt: En samtale beskyttet med kryptografi + en nøkkelinfrastruktur som kobler nøkler til personer.

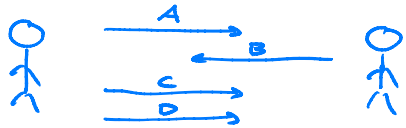
Sikkerhet er at angriperen ikke får gjort det han vil.

- Bare personene i samtalen vet hva som ble sagt.
- Begge parter er enige om hva som er sagt, i hvilken rekkefølge. Og *hvem det er sagt til*.

EU-forordning Nr. 910/2014, Artikel 8, 2 b):

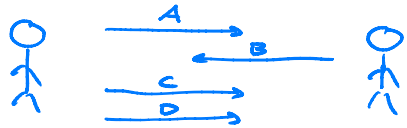
- sikringsniveauet *»betydelig«* henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der udviser en middelstor grad af tillid til en persons påståede identitet [...]

To observasjoner



Kryptologi har vært et fantastisk vellykket prosjekt over de fire siste tiårene.

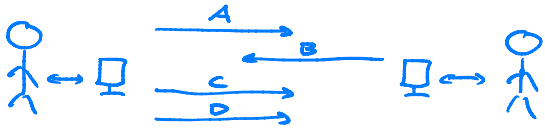
To observasjoner



Kryptologi har vært et fantastisk vellykket prosjekt over de fire siste tiårene.

Mennesker gjør ikke krypto.

To observasjoner

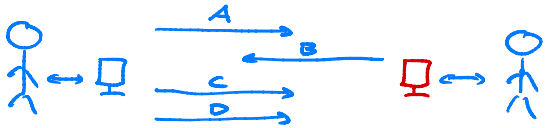


Kryptologi har vært et fantastisk vellykket prosjekt over de fire siste tiårene.

Mennesker gjør ikke krypto.

Dingser gjør krypto.

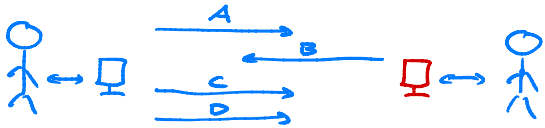
Bredere trusselbilde



Hvis datamaskinen din har signeringsnøkkelen din og noen bryter seg inn på datamaskinen din, da kan de signere hva som helst.

- Smartkort, sikre elementer, o.l. forhindrer tyveri av nøkkelen.

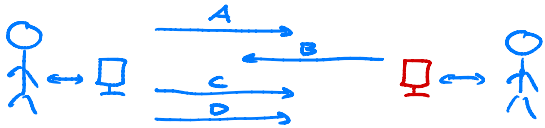
Bredere trusselbilde



Hvis datamaskinen din har signeringsnøkkelen din og noen bryter seg inn på datamaskinen din, da kan de signere hva som helst.

- Smartkort, sikre elementer, o.l. forhindrer tyveri av nøkkelen.
- OBS! Ingen er interessert i nøkler. Angriperen er fornøyd om han får brukt nøkkelen.

Bredere trusselbilde



Hvis datamaskinen din har signeringsnøkkelen din og noen bryter seg inn på datamaskinen din, da kan de signere hva som helst.

- Smartkort, sikre elementer, o.l. forhindrer tyveri av nøkkelen.
- OBS! Ingen er interessert i nøkler. Angriperen er fornøyd om han får brukt nøkkelen.

Det har vært vanskelig å ta i bruk naive kryptoløsninger.

Andre løsninger

Vi kan bruke *tiltrodde tredjeparter* mer aktivt.

- Bob spør Ted om det virkelig er Alice som vil snakke.
- Alice overbeviser Ted om at hun vil snakke med Bob.
  - Alice gir Ted en *engangskode* fra en *dings*.
  - Alice gir Ted et *passord*.
- Deretter går Ted god for Alice overfor Bob.

Andre løsninger

Vi kan bruke *tiltrodde tredjeparter* mer aktivt.

- Bob spør Ted om det virkelig er Alice som vil snakke.
- Alice overbeviser Ted om at hun vil snakke med Bob.
  - Alice gir Ted en *engangskode* fra en *dings*.
  - Alice gir Ted et *passord*.
- Deretter går Ted god for Alice overfor Bob.

Hvorfor tror Bob at han snakker med Alice?

- Bob vet at Ted sier at det er Alice.

Andre løsninger

Vi kan bruke *tiltrodde tredjeparter* mer aktivt.

- Bob spør Ted om det virkelig er Alice som vil snakke.
- Alice overbeviser Ted om at hun vil snakke med Bob.
  - Alice gir Ted en *engangskode* fra en *dings*.
  - Alice gir Ted et *passord*.
- Deretter går Ted god for Alice overfor Bob.

Hvorfor tror Ted at han snakker med Alice?

- Ted vet at en dings som er utstedt til Alice har laget en kode.
  - Hvis Alice alltid har kontroll på dingsene utstedt til henne, så har Alice laget en kode.

Andre løsninger

Vi kan bruke *tiltrodde tredjeparter* mer aktivt.

- Bob spør Ted om det virkelig er Alice som vil snakke.
- Alice overbeviser Ted om at hun vil snakke med Bob.
  - Alice gir Ted en *engangskode* fra en *dings*.
  - Alice gir Ted et *passord*.
- Deretter går Ted god for Alice overfor Bob.

Hvorfor tror Ted at han snakker med Alice?

- Ted vet at Alice sitt passord ble oppgitt.
  - Hvis bare Alice kjenner passordet, så har Alice oppgitt passordet «på et vis».

Andre løsninger

Vi kan bruke *tiltrodde tredjeparter* mer aktivt.

- Bob spør Ted om det virkelig er Alice som vil snakke.
- Alice overbeviser Ted om at hun vil snakke med Bob.
  - Alice gir Ted en *engangskode* fra en *dings*.
  - Alice gir Ted et *passord*.
- Deretter går Ted god for Alice overfor Bob.

Hvorfor tror Ted at han snakker med Alice?

- Ted vet ikke kryptografisk at Alice ønsker å snakke med Bob.
  - Hvis Alice sin datamaskin er ærlig, da har datamaskinen fortalt Alice at hun snakker med Bob.

Nye nye løsninger: Biometri

Biometri kan brukes riktig. Biometri kan brukes feil.

- Kan det kopieres?

Nye nye løsninger: Biometri

Biometri kan brukes riktig. Biometri kan brukes feil.

- Kan det kopieres?
- Har vi kontroll på sensoren?

Nye nye løsninger: Biometri

Biometri kan brukes riktig. Biometri kan brukes feil.

- Kan det kopieres?
- Har vi kontroll på sensoren?
- Er sensoren en del av en dings brukeren har kontroll på?

Spørsmål?