



Denne forelesningsøkten vil bli tatt opp og lagt ut i emnet i etterkant.

Hvis du ikke vil være med på opptaket:

	La være å delta med webkameraet ditt.
	La være å delta med mikrofonen din.
To: Marianne Sundby (Privately) Type message here...	Still spørsmål i Chat i stedet for som lyd. Hvis du ønsker kan spørsmålet også sendes privat til foreleser.



Høyskolen
Kristiania

TK2100: Informasjonsikkerhet

Første forelesning

Bengt Østby

Om Bengt Østby

- C-programmerer og Etisk hacker
- Windows system drivere
- 16 års erfaring fra anti-virus bransjen
- Jobbet med avansert video overvåking
- Brutt meg inn hos banker og i kritisk infrastruktur
- Lead Programmer, Norman
- Enterprise Architect Security CoE, AVG
- Security Concepts Group
- Head of Offensive Security, Capgemini Cybersecurity
- Nordic lead Advanced Attack and Readiness Operations, ACN
- Foreleser Høyskolen Kristiania (og USN)
- Senior Teknolog - Stortinget



Lærebok og pensum

- Michael T. Goodrich & Roberto Tamassia: *Introduction to Computer Security* (2011)

eller

- International Edition (ISBN 978-0-321-70201-2) (2014)
 - Samme bok, men mangler ett kapittel og har litt annen rekkefølge på dem

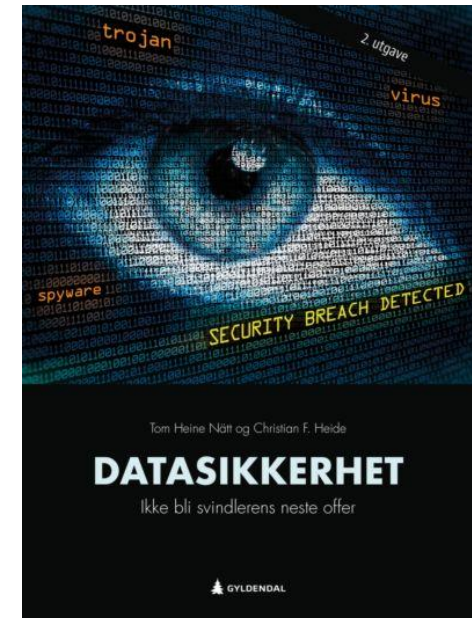
- Christian F. Heide, Tom Heine Nätt: *Datasikkerhet* (2021)

- Slider til forelesning

- Slidene er veldig detaljerte og kan fungere som et kompendium i seg selv
- Slider som går veldig i dybden, eller temaer som er utenfor kjernepensum, er merket med en stjerne – hvis du sliter med å henge med hopper du over dette, hvis ikke så er dette også stoff du burde sette deg inn i ☺



- Diverse linker og artikler i Canvas



Lærebok og pensum

- Michael T. Goodrich & Roberto Tamassia: *Introduction to Computer Security* (2011)
- International Edition (ISBN 978-0-321-70201-2) (2014)
- Faglig sterk bok på de grunnleggende emnene som malware og kryptering
- Boken er fra 2011 og ikke oppdatert på siste «trender»

- Kjøp e-bok Adlibris (560 kroner)

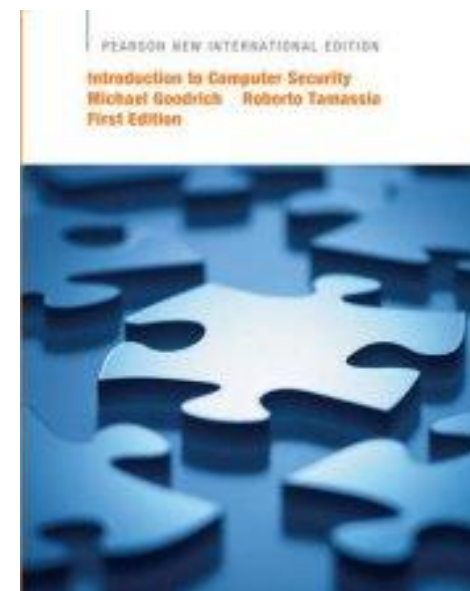
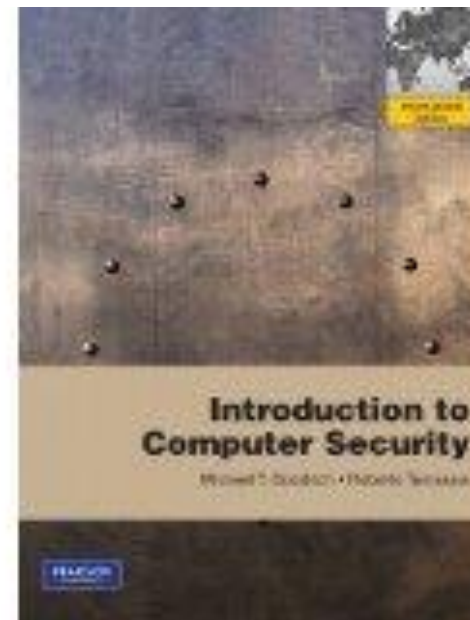
<https://www.adlibris.com/no/e-bok/introduction-to-computer-security-pearson-new-international-edition-pdf-ebook-9781292037912>

- LEIE som e-bok Akademika 180 dager (299 kroner)

<https://www.akademika.no/introduction-computer-security-pearson-new-international-edition/tamassia-michael-goodrich-roberto>

eller - Kjøp fysisk fra Amazon eller forskjellige bruktkanaler (finn.no)

<https://www.amazon.com/Introduction-Computer-Security-Goodrich-Paperback/dp/B011YUP8CO>

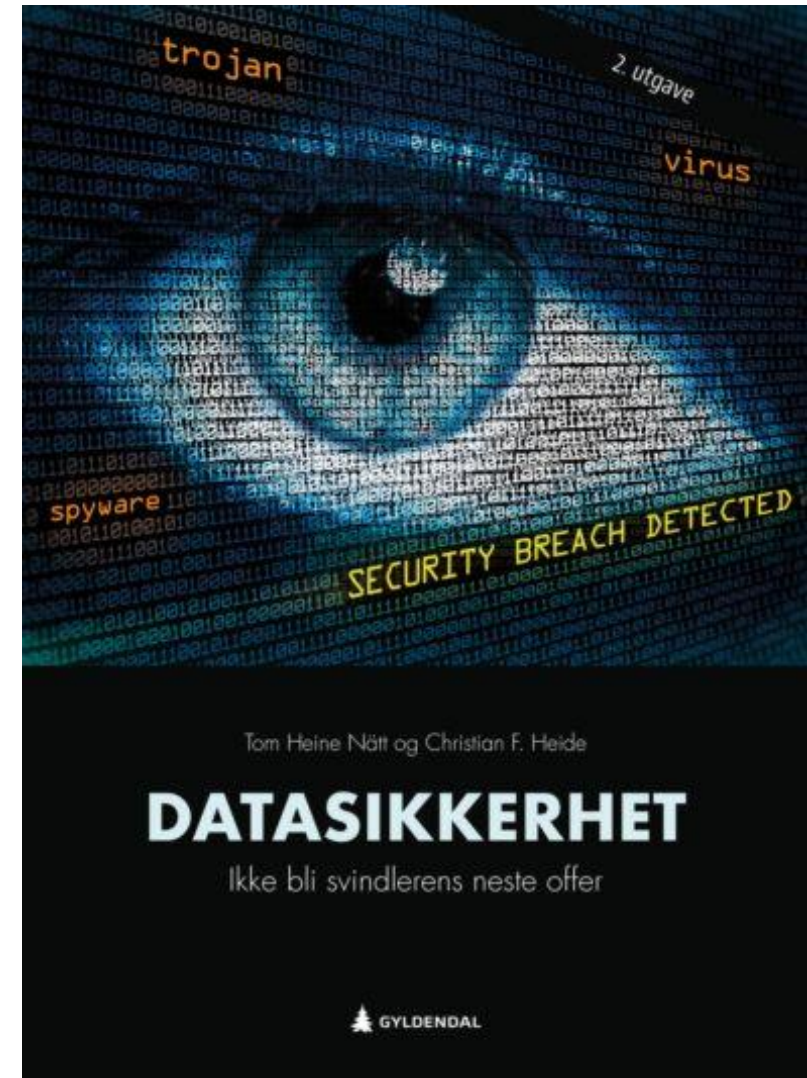


Lærebok og pensum

- Christian F. Heide, Tom Heine Nätt:
Datasikkerhet (2021)
- Helt oppdatert bok, pedagogisk
- Skrevet av norske forfattere
- Er ikke så teknisk, og mangler noe av det tekniske fra pensum som kryptering (derav fortsatt behov for den andre pensumboken)

Norli, ARK Bokhandel, Adlibris, mfl (499 kroner)

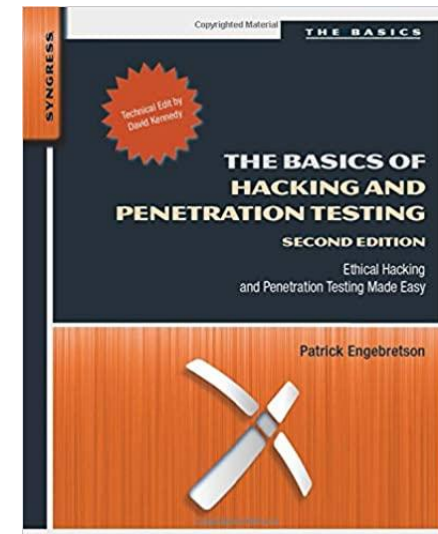
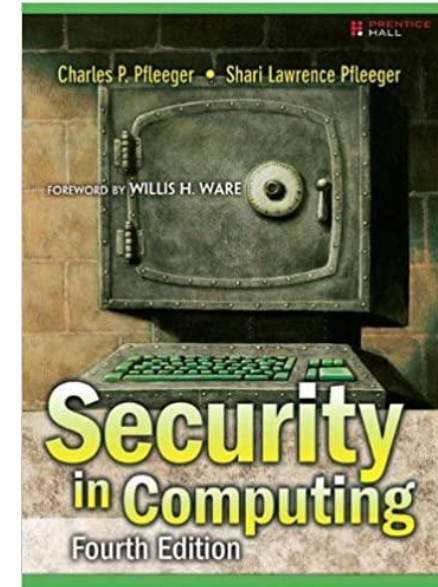
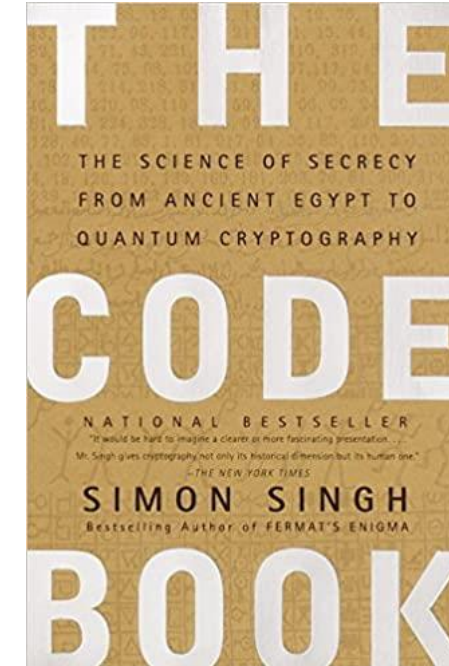
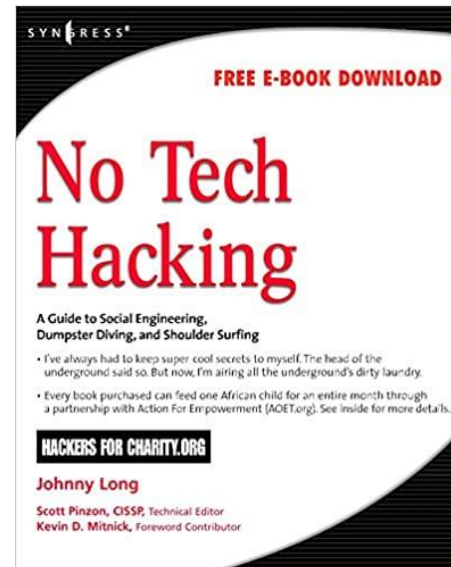
<https://www.norli.no/datasikkerhet-2>





Annen litteratur

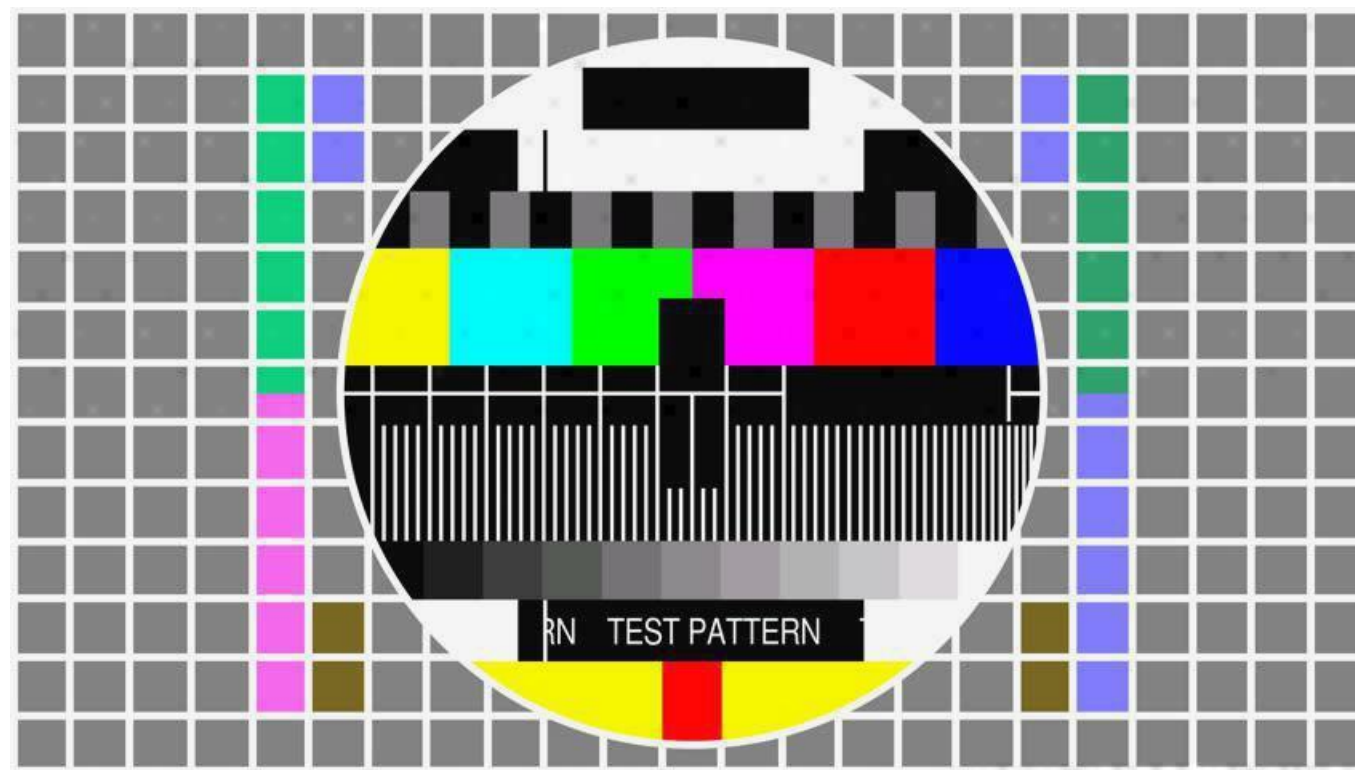
- Security in Computing, Pfleeger
- The Codebook, Simon Singh
- No Tech Hacking, Johnny Long
- The basics of Hacking And Penetration testing



Hva skal vi lære?

- Hva er informasjonssikkerhet?
 - Definisjoner/begreper og modeller
 - Teknikker og verktøy
 - Prosedyrer og rutiner
 - Sikkerhetsvurderinger
- Hvordan beskytte seg selv
 - Trusselbildet pr i dag
 - Kryptering
 - Sikkerhetsmekanismer og policies
- Lov og rett
 - Hvilke regler gjelder mhp opphavsrett og personvern.
 - Hvordan er norsk forskjellig fra amerikansk?

Hva er dette?



- **Steganografi**
 - Det er gjemt en melding inne i bildet...

Sett sånne?

Hilsener! Spam x



zhongjun@asia.com

to Recipients ▾

30/12/2015 (7 days ago) ☆



⚠ Be careful with this message. Similar messages have been used to steal people's personal information. Unless you trust the sender, don't click on links or reply with personal information. [Learn more](#)

Komplement av sesongen!

Jeg trenger en utenlandsk partner for en foreslått gjensidig virksomhet, som refererer til overføring av en stor sum penger til en konto i utlandet, som mottaker av midlene. Alt om denne operasjonen, vil være lovlig gjøres uten noen bro økonomisk autoritet, både i mitt land og yours. I wil hengi deg utvise den ytterste skjønn i alle saker som angår denne saken. Hvis du er interessert, kan du svare tilbake gjennom min private e-postadresse er skrevet ned, jeg skal gi deg mer informasjon om meg selv med finansinstitusjonen jeg representert og de faktiske beløpene som er involvert om prosjektet så jeg får positiv respons.

Private E-post: fzhongjun@yahoo.com.hk

Vennlig hilsen,

Daglig leder.

- Phishing (eller ren svindel/scam)

Hvor kommer uttrykket «SPAM» fra?



Så hva skal vi lære?

- Kryptering
 - Hvordan, når og hvor sterk
- Sikkerhet i OS
 - Hvilke mekanismer er i bruk, og hvor gode er de egentlig?
- Malware
 - Typer, hvor farlige?
- Nettverk
 - Sniffing, ARP-spoofing, portscanning, session-hijacking, DDoS-angrep ...
- WWW
 - SQL Injection, XSScripting, ...

Kurs-opplegget

- 12 leksjoner med 2 timer undervisning og 2 timer veiledet øving
 - Delt klasse (som i TK1104), en gruppe 08.15 – 12.00, og en gruppe 13.15 – 17.00
 - Studenter i Bergen følger forelesning digitalt – 13.15 forelesningen streames
 - I Oslo er forelesningene i auditoriet T34 TAU-201
 - Øvingstimene i Oslo er i NAR-200 (primært), evt har vi reservert A2-10 og A2-12
- **HUSK AT egenarbeid** er VIKTIG (aktiviser kunnskap!)

Oversikt over forelesninger

- Introduksjon til sikkerhet (11. januar)
- 1: Kryptering (18. januar)
- 2: Operativsystemet (25. januar)
- 3: Malware (1. februar)
- 4: Verdens farligste virus (8. februar)
- 5: Web sikkerhet (1. mars)
- 6: Nettverkssikkerhet I (8. mars)
- 7: Nettverkssikkerhet II, Internet of Things (15. mars)
- 8: Modeller, lover, pentesting (22. mars)
- 9: Opphavsrett, DRM, spam (5. april)
- 10: Defensive Programming (19. april)
- 11: Oppsummering (26. april)
- Eksamen

Vurdering 2022

- 24 timers hjemmeksamen
 - Individuell
 - Bestått / ikke bestått
- Arbeidskrav: Fritekstoppgave
 - Individuell
 - Oppgavetekst kommer 8. februar

Trusselbildet

«Sikkerhet er alltid i forhold til et trusselbilde.»

Den «gamle» fienden



Chen-Ing Hau
CIH Virus



Joseph McElroy
Hacked US Dept of Energy



Jeffrey Lee Parson
Blaster-B copycat

- «Datsnoker» og «script-kiddies» som gjorde det for spenning og «morro»

Malware 1991: Casino

DISK DESTROYER - A SOUVENIR OF MALTA

I have just DESTROYED the FAT on your Disk !!

However, I have a copy in RAM, and I'm giving you a last chance
to restore your precious data.

WARNING: IF YOU RESET NOW, ALL YOUR DATA WILL BE LOST - FOREVER !!

Your Data depends on a game of JACKPOT

CASINO DE MALTE JACKPOT

CREDITS: 5

any key to play

Fienden i 2015



Jeremy Jaynes
\$24M SPAM KING



Jay Echouafni
Competitive DDoS



Andrew Schwarmkoff
Russian Mob Phisher

- De er ute etter:
 - maskinen din (f.eks. botnet)
 - identiteten din (for å få fatt i ...)
 - *pengene* dine.

Malware 2013: Ransom-ware

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

- Programvare som benytter assymetrisk kryptering til å gjøre alle dine data utilgjengelige for deg.

This computer lock is aimed to stop your illegal activity.

- «Tok av» med CryptoLocker i 2013

You have 72 hours to pay the fine otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.



OK

Fienden i 2019/2020


- De samme kriminelle aktører som de siste år, pluss noen enda skumlere aktører:



- De er ute etter:
 - Meningene dine
 - Innflytelse over livet ditt
 - Stemmen din neste valg

Cyberwar ala 2016

- Innbrudd i epost servere
- Utro tjenere / lekkasjer
- Hva er fake news, og hva er ekte?



The screenshot shows a web browser window with the address bar displaying <https://wikileaks.org/clinton-emails/>. The WikiLeaks logo is visible on the left, with navigation links for Leaks, News, About, and Partners. The main heading is "Hillary Clinton Email Archive". Below this, a paragraph of text describes the archive: "On March 16, 2016 WikiLeaks launched a searchable archive for over 30 thousand emails & email attachments sent to and from Hillary Clinton's private email server while she was Secretary of State. The 50,547 pages of documents span from 30 June 2010 to 12 August 2014. 7,570 of the documents were sent by Hillary Clinton. The emails were made available in the form of thousands of PDFs by the US State Department as a result of a Freedom of Information Act request. The final PDFs were made available on February 29, 2016." At the bottom, there are two search input fields: "Search by Terms in Email" and "Search by Email-ID".

← → ↻ <https://wikileaks.org/clinton-emails/>

 WikiLeaks Leaks News About Partners

Hillary Clinton Email Archive

On March 16, 2016 WikiLeaks launched a searchable archive for over 30 thousand emails & email attachments sent to and from Hillary Clinton's private email server while she was Secretary of State. The 50,547 pages of documents span from 30 June 2010 to 12 August 2014. 7,570 of the documents were sent by Hillary Clinton. The emails were made available in the form of thousands of PDFs by the US State Department as a result of a Freedom of Information Act request. The final PDFs were made available on February 29, 2016.

Search by Terms in Email Search by Email-ID

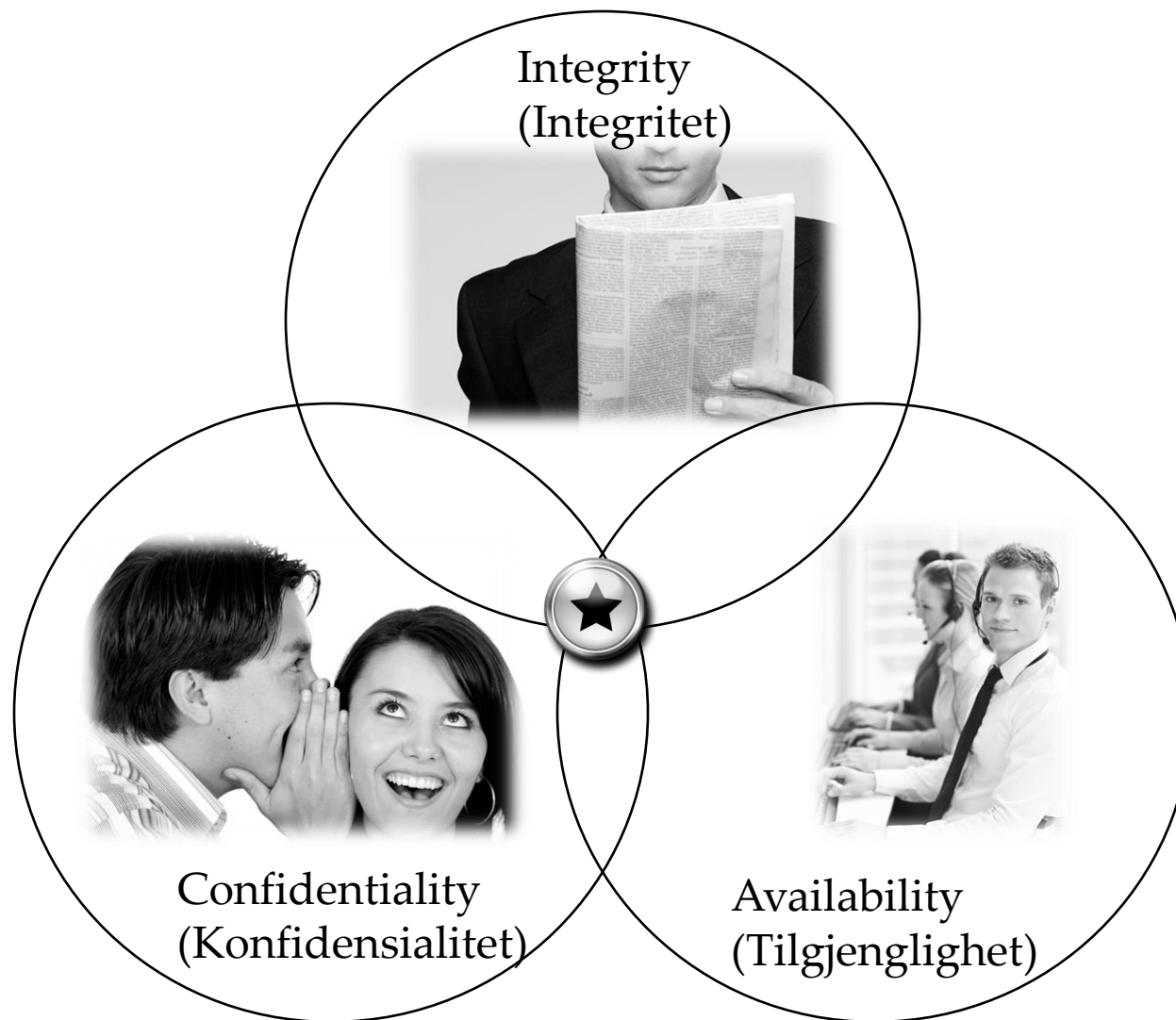
CIA

Modeller for å analysere hva sikkerhet går ut på.

Hva er informasjonsikkerhet?

- Et system, en applikasjon, eller protokoll er bare **sikker** i forhold til:
 - Forhåndsdefinerte, ønskede egenskaper
 - En motstander med spesifiserte evner og egenskaper
- Sikkerhet er alltid i forhold til et **trusselbilde**
- For eksempel:
 - Tilgangen til en Windows maskin er ikke sikkert for den som har fysisk tilgang til den og kan boote den.
 - Se f.eks. <http://pogostick.net/~pnh/ntpasswd/>

- C.I.A.

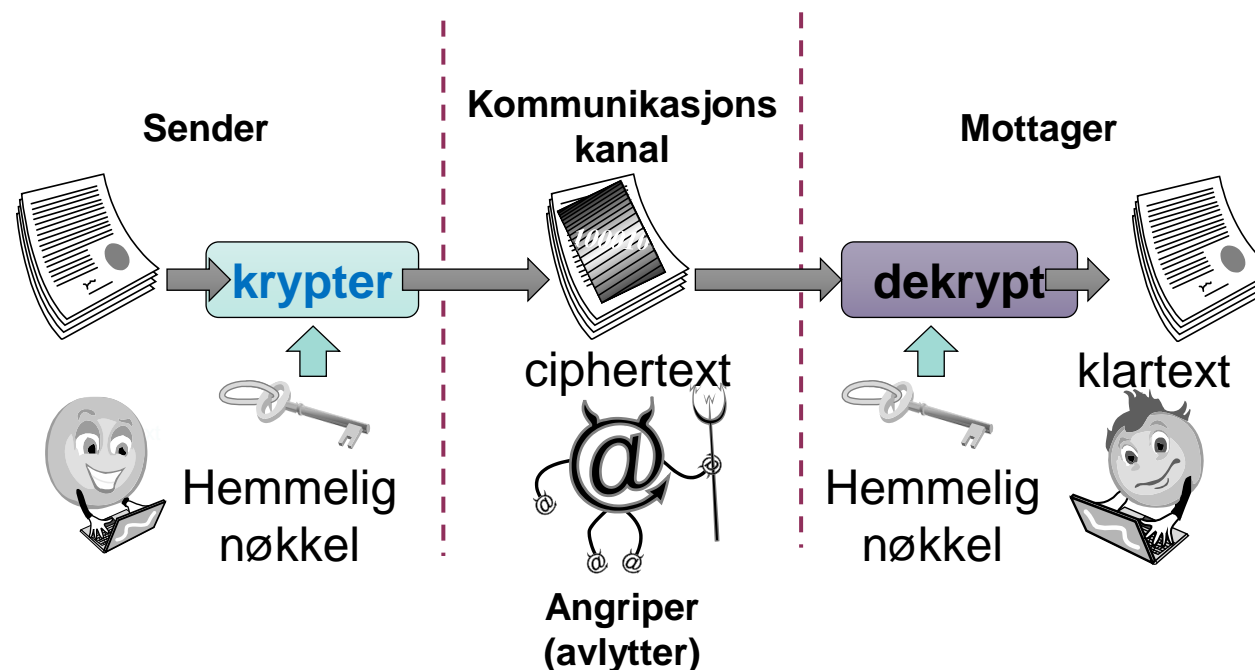


- **Konfidensialitet** er å *unngå uautorisert* tilgjengliggjøring av informasjon
 - Beskytte data
 - Kun gi adgang til de som har fått tillatelse
 - Sperre alle andre fra å lære noe som helst om dataene

Konfidensialitet verktøy 1

Kryptering: Omgjøringen (transformasjon) av informasjon v.hj.av en *hemmelighet* (**krypteringsnøkkel**), slik at den krypterte meldingen (**chifferskrift**) bare kan leses/ses med hjelp av en annen hemmelighet (**dekrypteringsnøkkelen**)

- Kryptering- og dekrypteringsnøkkel kan, men må ikke, være like.



Konfidensialitet verktøy 2

Adgangskontroll (Access control):

Regler og **retningslinjer** (“policy”) som **begrenser** adgangen til konfidensiell informasjon til de personene/systemene som **“trenger å vite”** (“need to know”).

- Gjelder både personer og datasystemer
- Kan reguleres ut fra identitet (navn), MAC-adresse, eller rolle (AD-server, Adm. dir., ansatt, ansatt-PC, systemansvarlig, ...)

Konfidensialitet verktøy 3

Autentisering

(Authentication):

Å avgjøre identiteten eller rollen til noen

- Kan gjøres på flere måter men er vanligvis basert på en kombinasjon av:
 - Noe en person **har**: smartkort, mobiltelefon, HW-nøkkel...
 - Noe en person **vet**: passord
 - Noe en person **er**: fingeravtrykk, iris.



Radiobrikke med nøkler

Noe du har

passord=uclb()w1V
mor=Godhjerta
årstall=1984



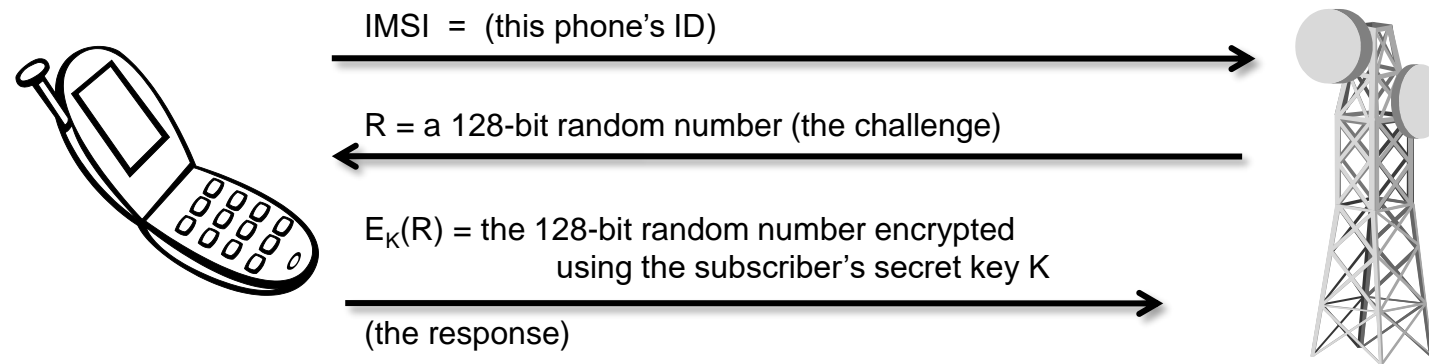
Noe du vet



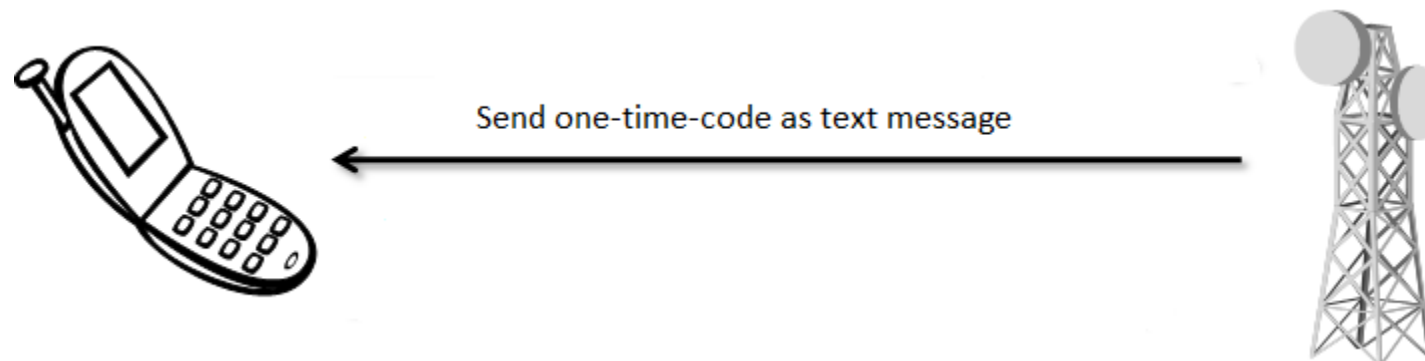
Menneske med
fingre og øyne

Noe du er

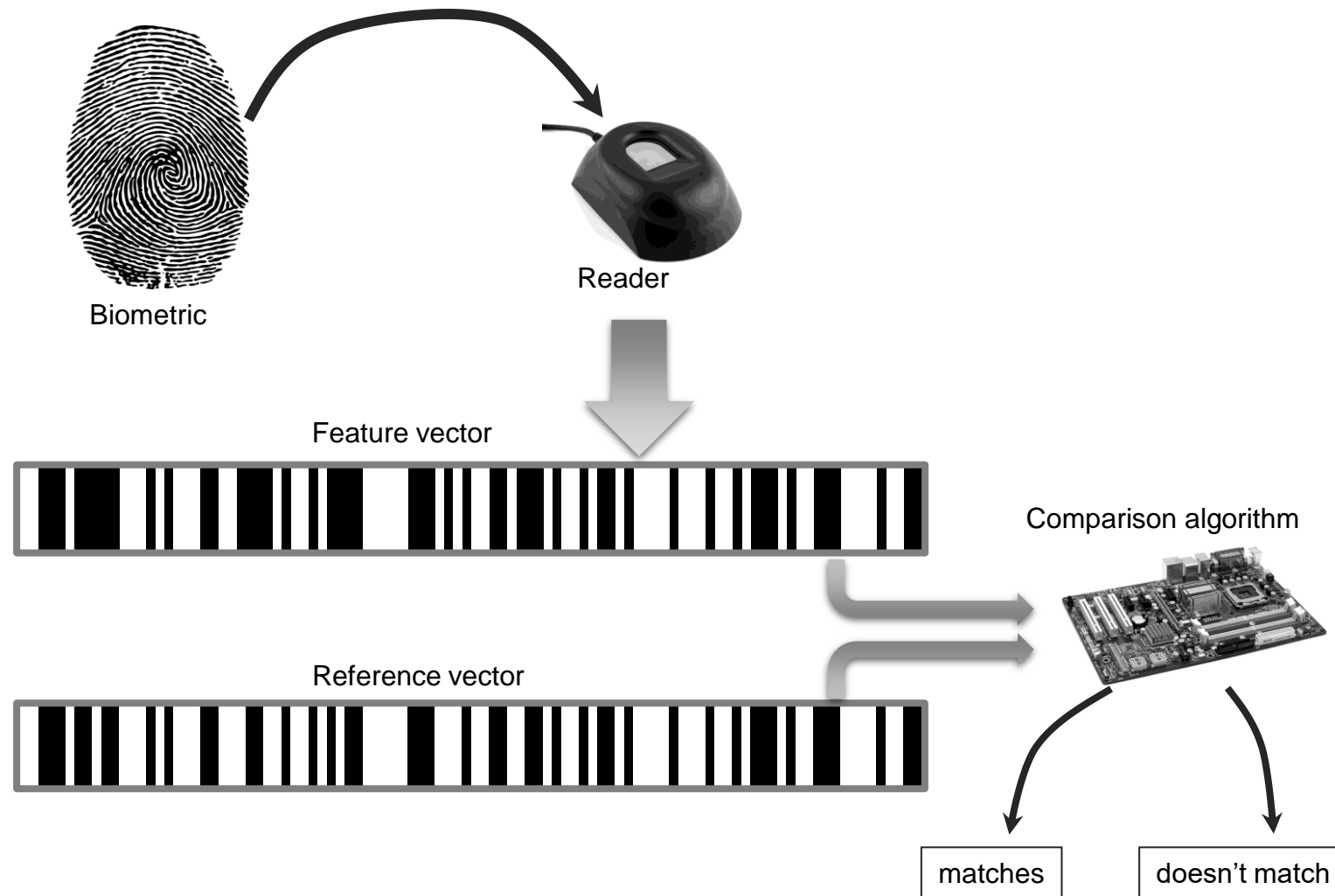
Ex: **To fase** autentisering med mobil



- Populært de siste årene
- Basert på noe du har...
- De fleste bruker den enkleste, men mindre sikre:



Fingeravtrykk



- Burde vært bra, men ikke så brukervennlig
- Kan ofte lures med et BILDE (eller modell) av et fingeravtrykk

Konfidensialitets-verktøy 4

Autorisering (Authorization):

å bestemme hvilke **ressurser** en person/system skal ha **tilgang** til, basert på **adgangs-retningslinjene**

- Bør forhindre angriperen fra å lure systemet til å gi ham adgang til beskyttede ressurser.

Fysisk sikring

å etablere fysiske barrierer som begrenser adgangen til beskyttede data-ressurser.

- Låser på dører (**jeg kan ikke understreke hvor viktig dette er!**)
- Plasser servere i rom *uten vindu*
- Lyddempende materialer
- Faraday-bur (radiobølge-isolasjon)

Integritet:

betyr at informasjon ikke har blitt endret på en uautorisert måte.

Verktøy:

- **Backup:** periodisk arkivering.
- **Sjekksummer:** Se TK1100 (CRC, paritetsbits)
Beregnes på grunnlag av all informasjonen som skal beskyttes og på en slik måte at selv små endringer resulterer i at sjekksummen ikke lenger samstemmer med informasjonen som skal beskyttes
- **Sjekksummer** kan også lages slik at uønskede endringer kan fjernes og opphavlig tilstand gjenopprettes

Tilgjengelighet (Availability)

Tilgjengelighet (Availability):

- at informasjon er tilgjengelig for, og mulig å endre innenfor rimelig tid av, de som er autorisert til det.

Andre begreper



- A.A.A.

Authenticity



Anonymity



Assurance

“Forsikring”/Assuranse (tillit)



Assuranse

handler om hvordan **tillit** etableres og administreres i datasystemer

Tillits-administrasjon baseres på:

- **Retningslinjer** (Policies)
 - spesifiserer forventet adferd fra folk og systemer
 - F.ex. iTunes spesifiserer hvordan brukere får adgang til og kan kopiere/dele åndsverk
 - Facebooks regler for hva som er akseptabel adferd og hva som kan publiseres
- **Tillatelser** (Permissions),
 - beskriver hva slags adferd som er **akseptabel/tillatt** for de som benytter systemet, eller samhandler med personer
 - F.ex iTunes dele-tillatelser innafor heimen når du har kjøpt en film/sang.
- **Beskyttelsesmekanismer**,
 - beskriver hvilke **mekanismer** som benyttes for å **håndheve retningslinjene** og tillatelsene
 - F.ex. Angiver-knappene i Facebook



- **Autentisitet**
er evnen til å fastslå om utsagn, retningslinjer, og tillatelser gitt av en person/ et system er ekte (ikke forfalsket)
- **Primær mekanisme:**
 - **digitale signaturer.**
Kryptografiske beregninger som tillater folk/systemer å forplikte seg på ektheten til f.eks. dokumenter på en slik måte at man ikke senere kan trekke forpliktelsen tilbake (**nonrepudiation**).



Anonymitet



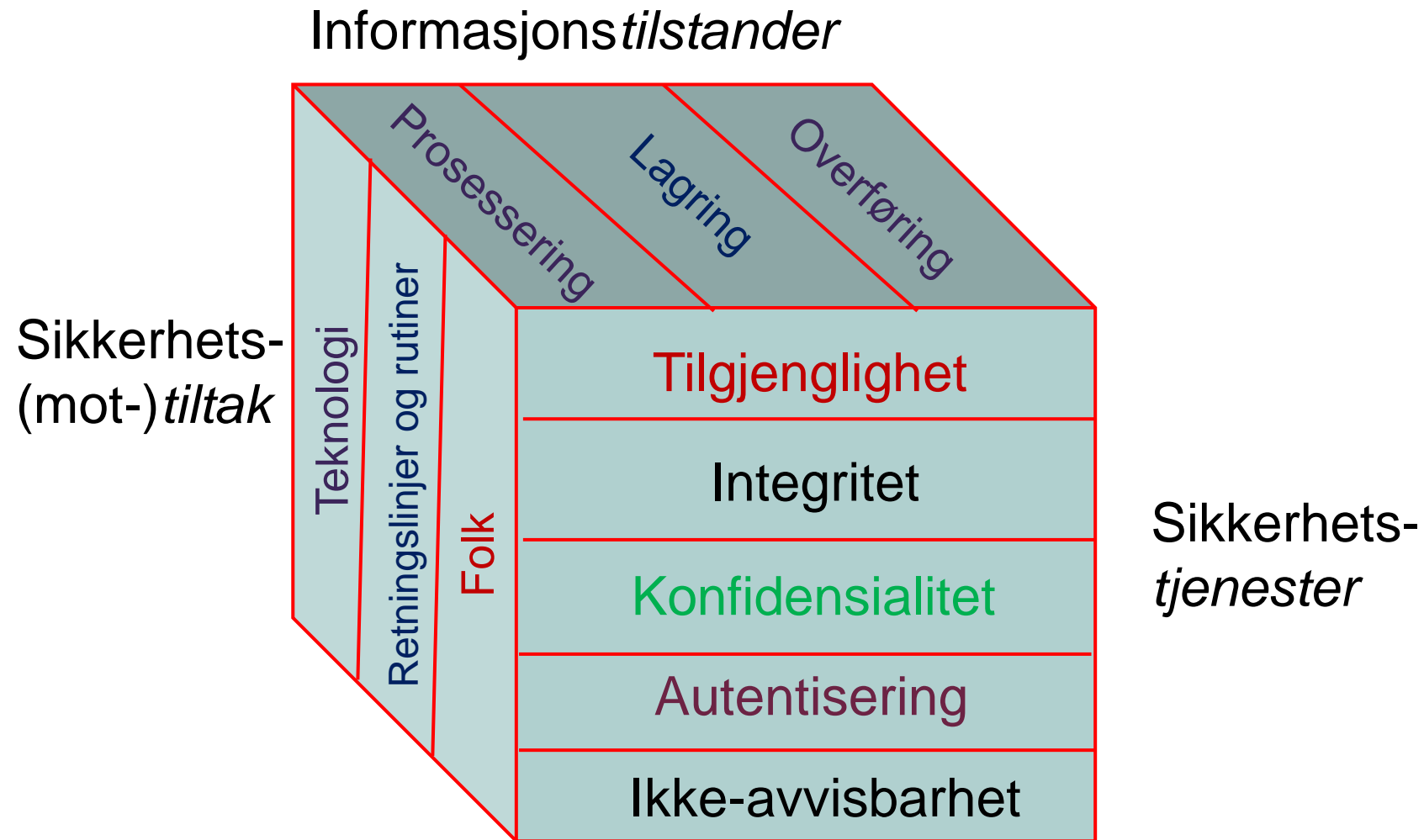
- **Anonymitet:**
at enkelte transaksjoner eller lagrede data **ikke** skal kunne **føres tilbake** til **et bestemt individ**.
- **Teknikker:**
 - **Aggregering:** kombinere individuelle data/spor på en slik måte at publiserte data umulig kan føres tilbake til noe individ.
 - **Mixing:** blande sammen attributter til “fiktive personer” oppstår.
 - **Proxy’er:** la noen/systemet handle på vegne av ekte individer på en måte som ikke kan spores tilbake.
 - **Pseudonym:** fiktiv identitet der ekte kun er kjent av systemet

Alternativ til CIA



- **CIA modellen** er i alle lærebøker og brukes aktivt i sikkerhetsbransjen i analyser og rapporter.
- Det finnes flere ulike **alternative** modeller
 - Felles er at de forsøker å være mer **finmaskede**...

IAM modellen



ACL o.l.

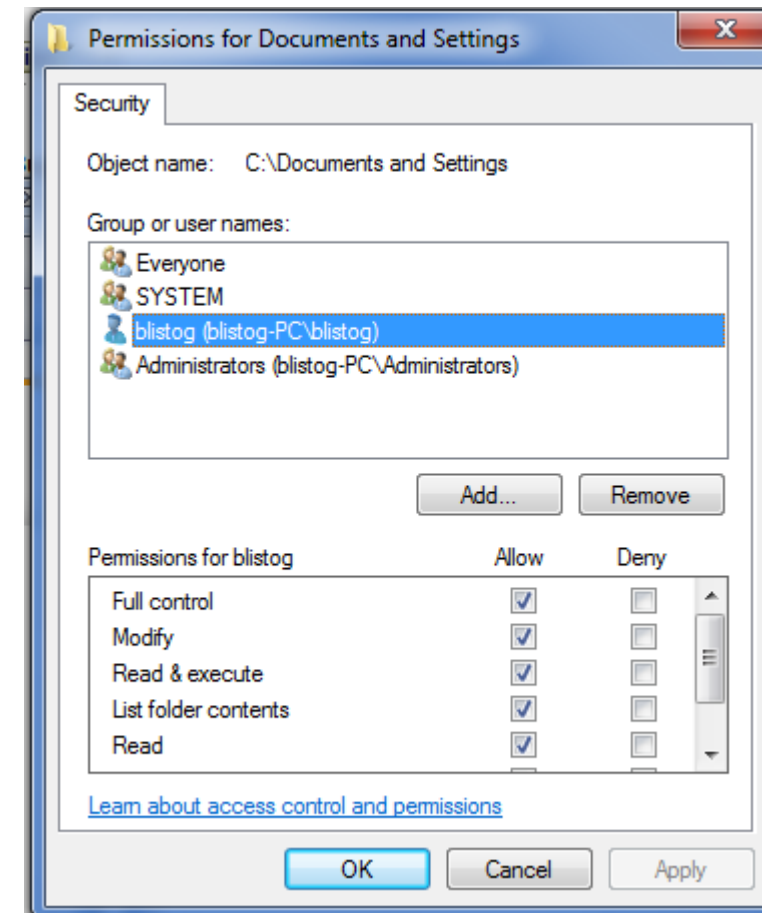
Teknikker for adgangsbegrensning

Emne: Access Control

- Brukere og grupper
 - Autentisering og autorisering
 - Passord
 - Fil-beskyttelse
 - Access control lister
- Hvilke brukere kan lese/skrive hvilke filer?
 - Er filene mine virkelig beskyttet?
 - Hva vil det si å ha root/Admin?
 - Hva ønsker vi egentlig å kontrollere?

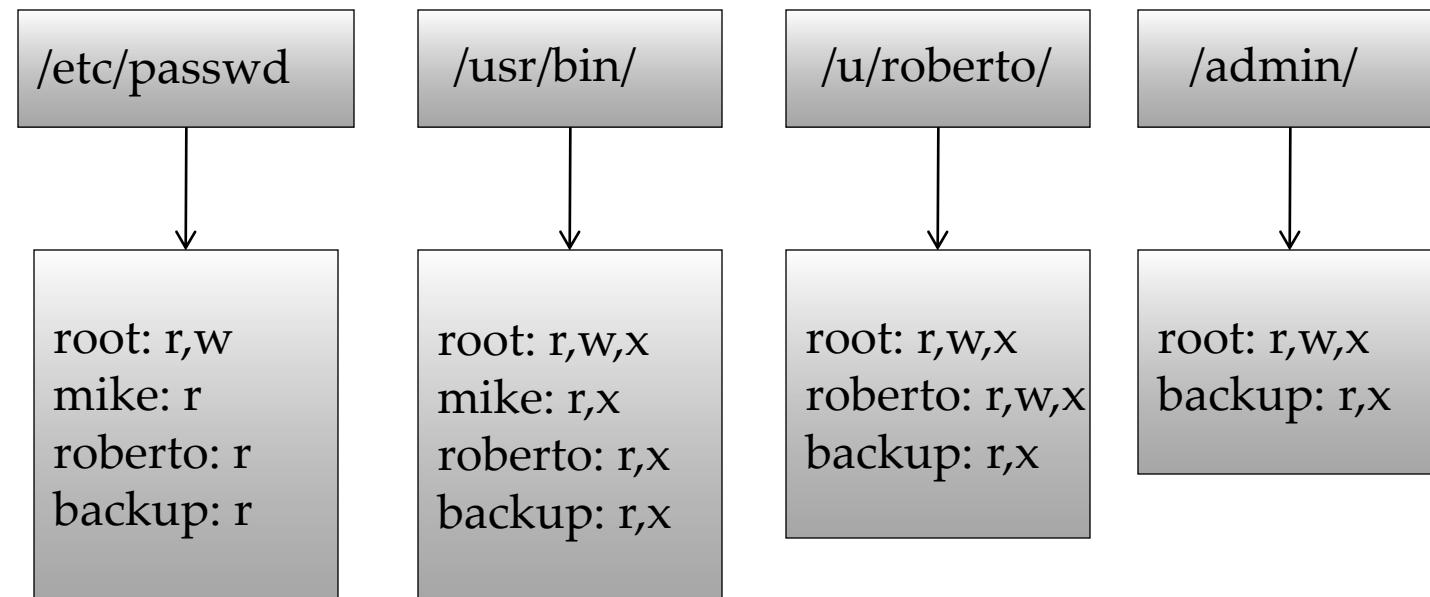
Access Control **Matriser**

- **En tabell som definerer tilgangsrettigheter.**
 - Hver rad er en bruker (gruppe, prosess eller service) som kan utføre handlinger.
 - Hver kolonne er assosiert med et objekt (fil, dokument, utstyr, ressurs,..) som vi vil bestemme adgangsrettigheter på.
 - Hver celle angir adgangsrettigheter for en kombinasjon av bruker og objekt/ressurs
 - Adgangsrettigheter kan være slikt som skrive, lese, eksekvere, slette, kopiere, ...
 - Tom celle betyr at det ikke er gitt rettigheter,



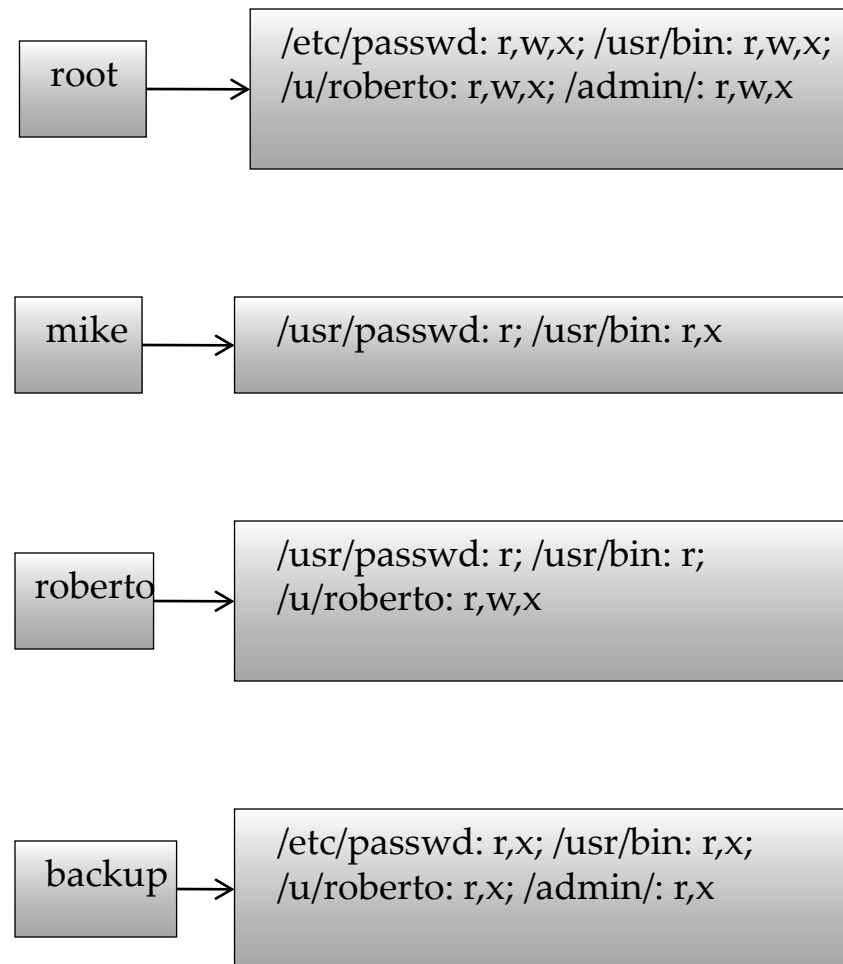
Access Control **List**

- Definerer for hvert objekt, **o**, en liste, **L**, som kalles **o's access control list**, den lister opp for alle brukere/prosesser om og hvilke rettigheter de har på **objektet**



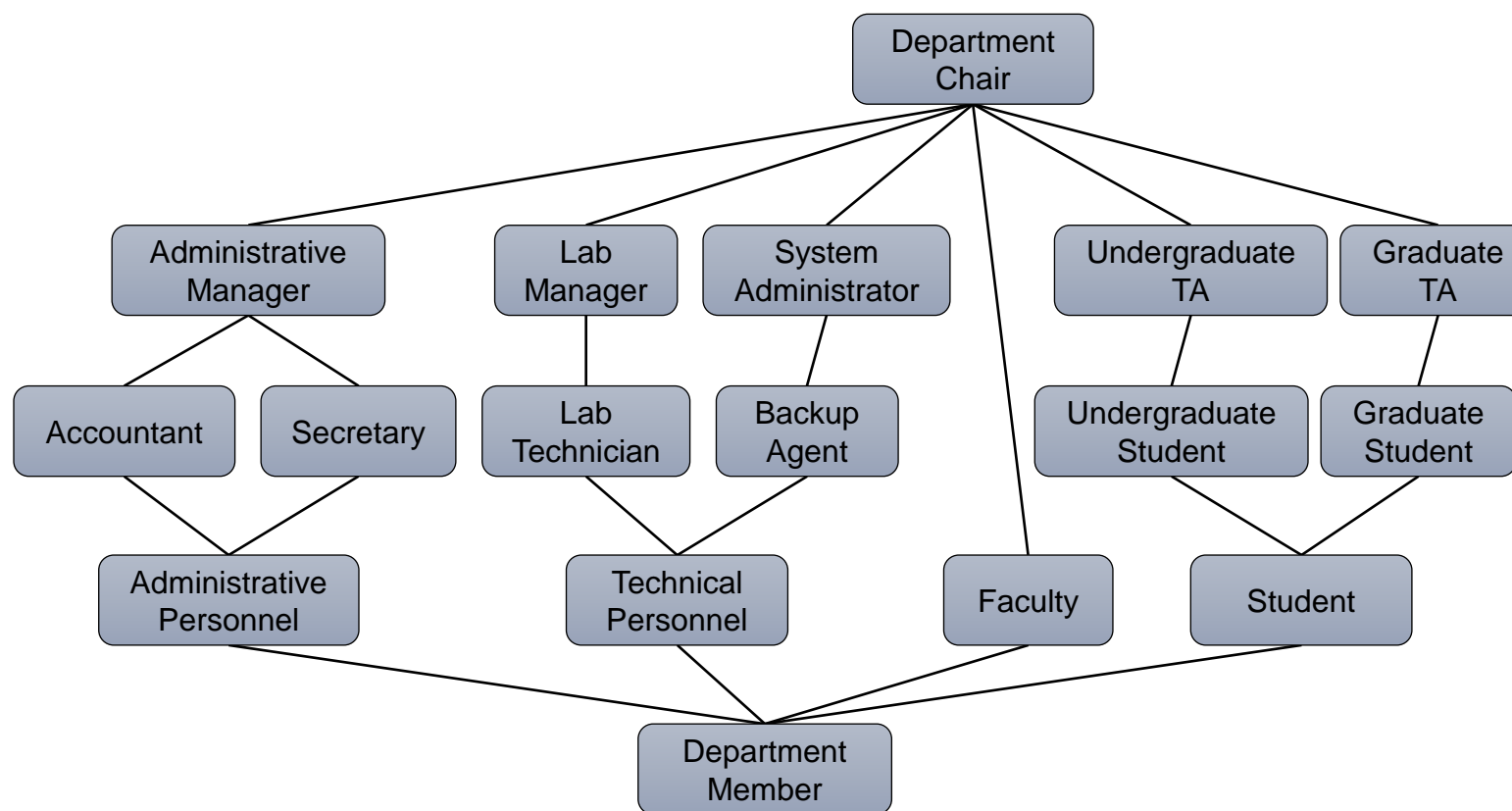
Capabilities

- Spesifiserer for hver **bruker/prosess** hvilke **ressurser** man/den har adgang til og hvilke **rettigheter**.
- Det “motsatte” av AC Liste.



Rolle-basert Access Control

- Definerer **roller** og spesifiserer adgangsrettigheter ut fra roller i stedet for enkeltbrukere direkte



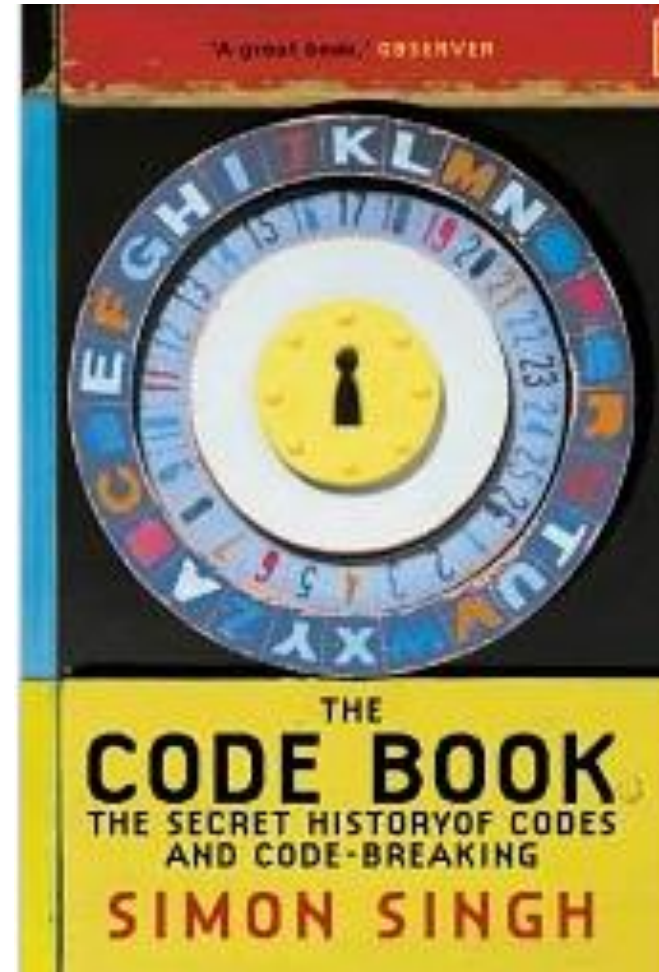
Kryptering

(Kort introduksjon)

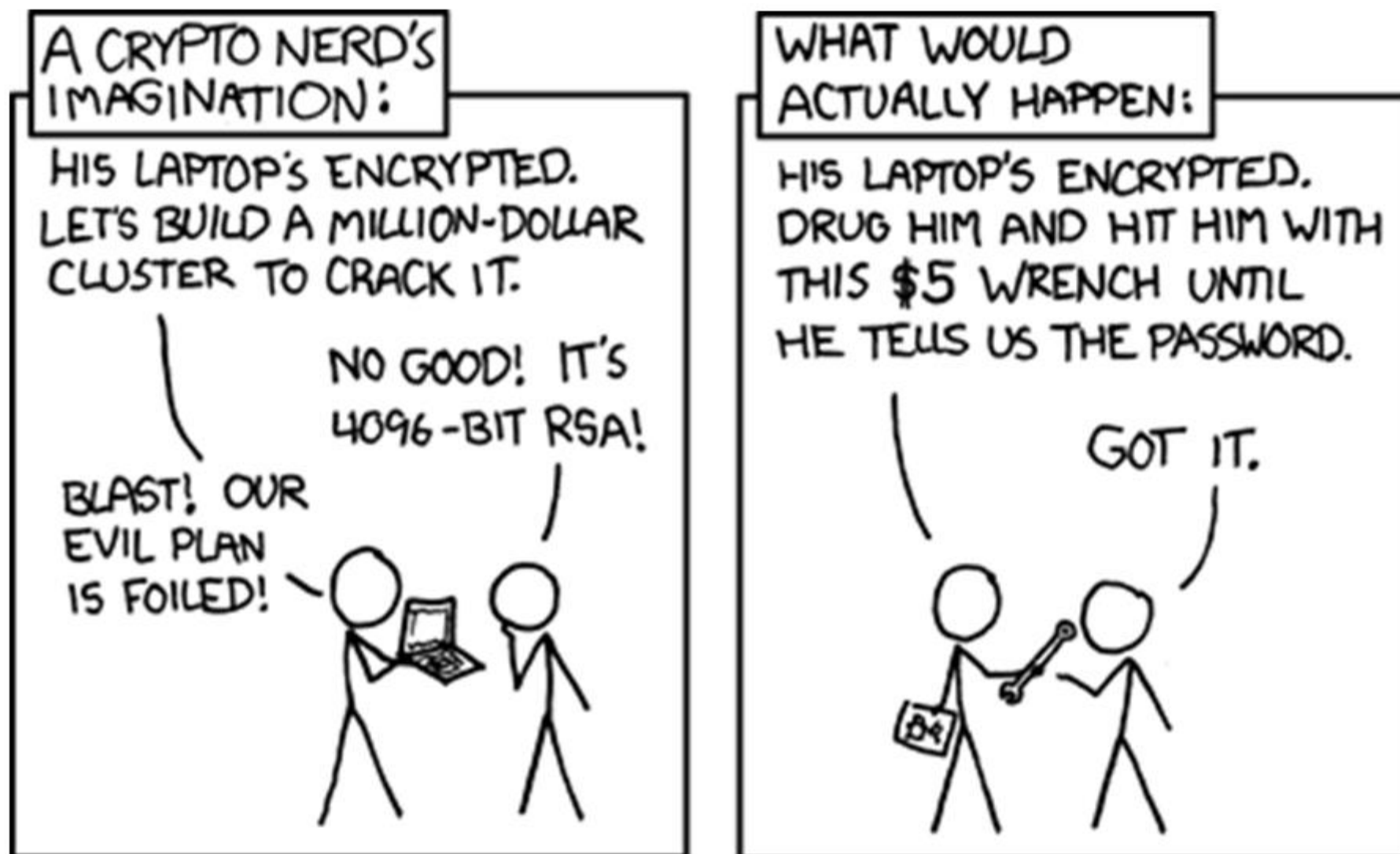
Boken **alle** bør lese

Simon Singh: *The Code Book*

- Finnes også i norsk utgave:
***Koder : skjulte budskap fra
det gamle Egypt til
kvantekryptografi***

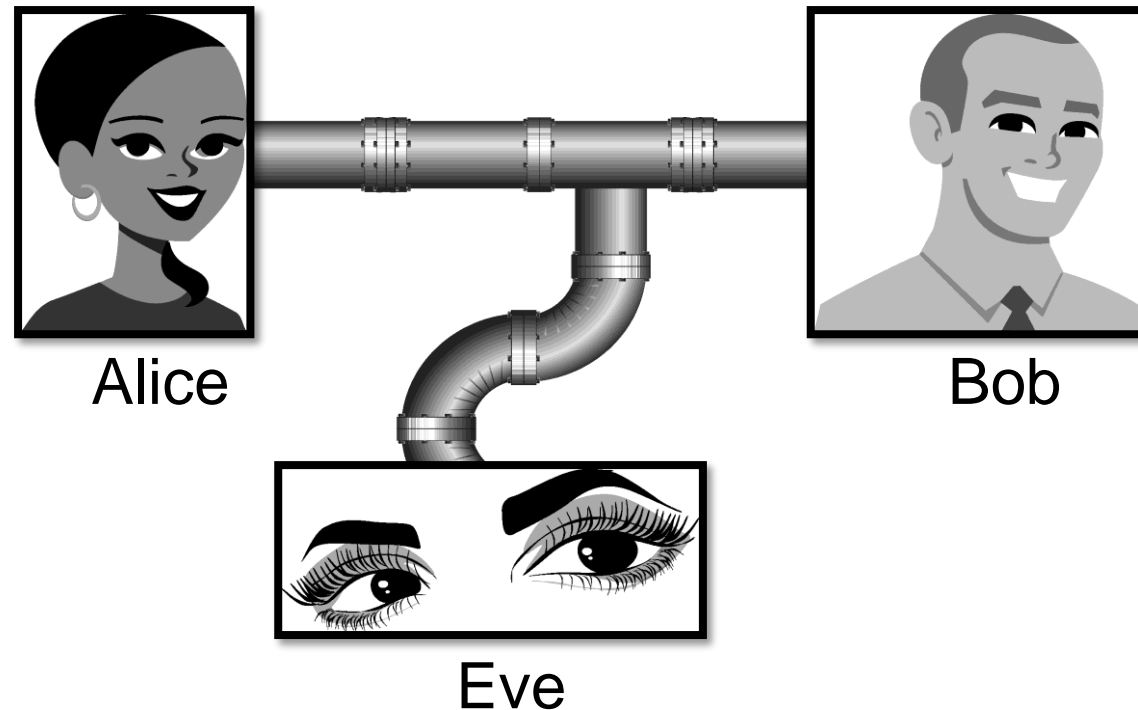


XKCDs kommentar



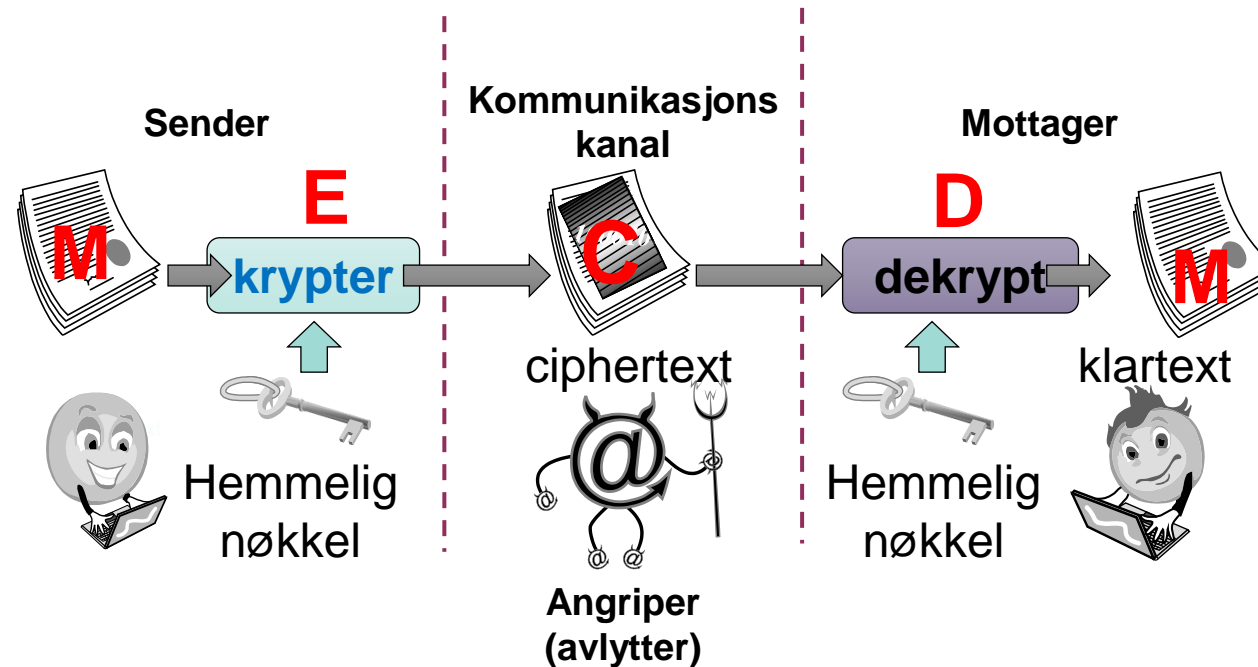
Kryptografiske **begrep**

- **Kryptering**: en måte å la to parter som litteraturen kalles Alice and Bob, utføre **konfidensiell kommunikasjon** over en **usikker kanal** som er gjenstand for avlytting (av Eve)



Kryptering og dekryptering

- Meldingen M kalles **klartext** (plaintext).
- Alice gjør om M til en chifertext C av M ved hjelp av krypteringsalgoritmen E .



Kryptering og dekryptering

- Ligninger/metoder:

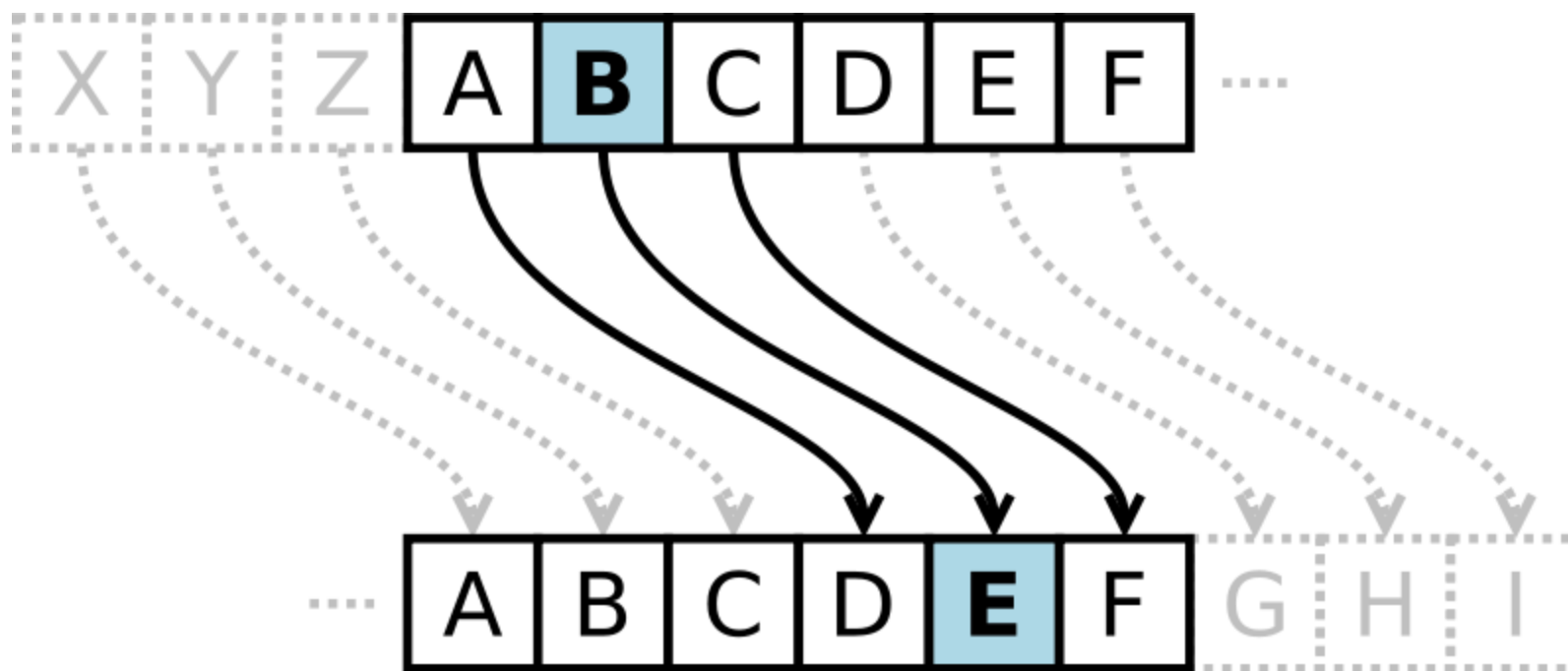
$$C = E(M)$$

$$M = D(C)$$

- Kryptering og dekryptering algoritmene velges slik at det ikke er gjennomførbart for andre enn Alice og Bob å finne klarteksten M ut fra chiferteksten C (uten ha nøkkelen(e))
- Dermed kan C overføres på en usikker kanal, selv om Eve avlytter den.

Cæsar Chipher

- Erstatt hver bokstav med den tre bortenfor
- Lett å knekke.



Krypto-analyse (lett=)

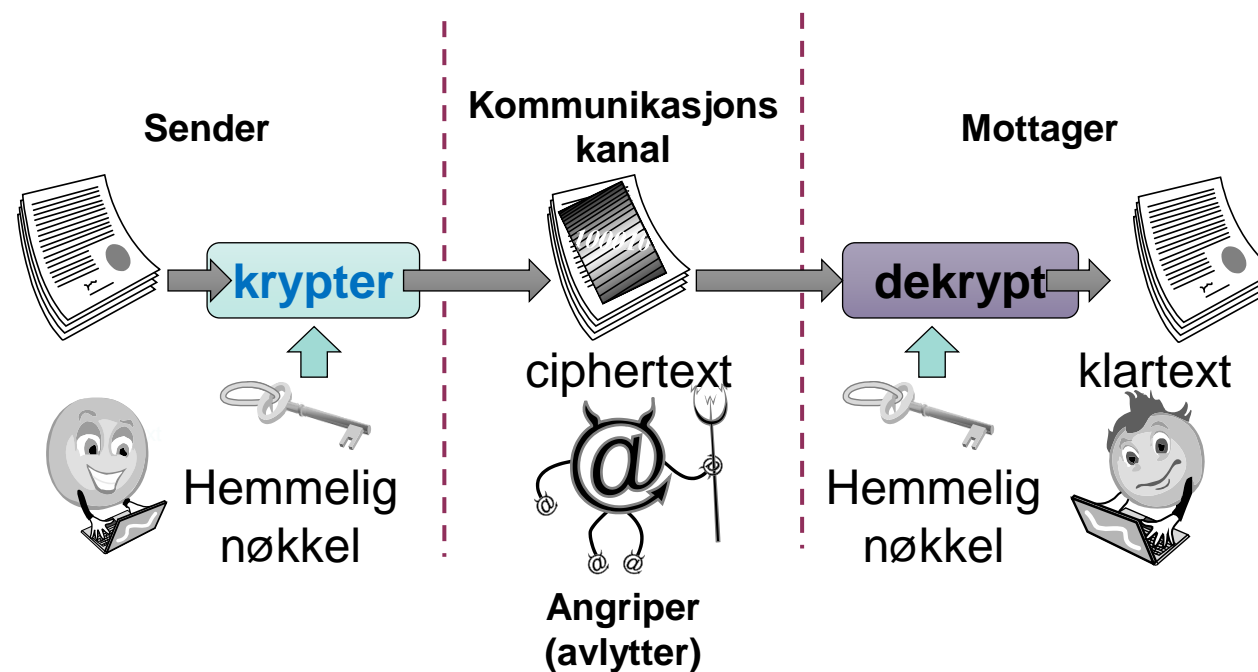
- Alle bokstaver brukes ikke like mye:

Bokstav	Frekvens	Bokstav	Frekvens	Bokstav	Frekvens	Bokstav	Frekvens	Bokstav	Frekvens	Bokstav	Frekvens
a	4,9%	f	1,7%	k	2,9%	p	1,2%	u	1,3%	z	0,0%
b	1,6%	g	3,0%	l	4,6%	q	0,0%	v	1,9%	æ	0,2%
c	0,15%	h	1,0%	m	2,5%	r	6,3%	w	0,0%	ø	0,7%
d	2,8%	i	4,7%	n	5,6%	s	5,8%	x	0,0%	å	2,0%
e	11,5%	j	0,9%	o	4,1%	t	6,5%	y	0,4%		

- I tillegg er noen kombinasjoner mye vanligere enn andre.
- Både Cæsar og substitusjon-chifre er dermed sårbare for frekvensanalyse.

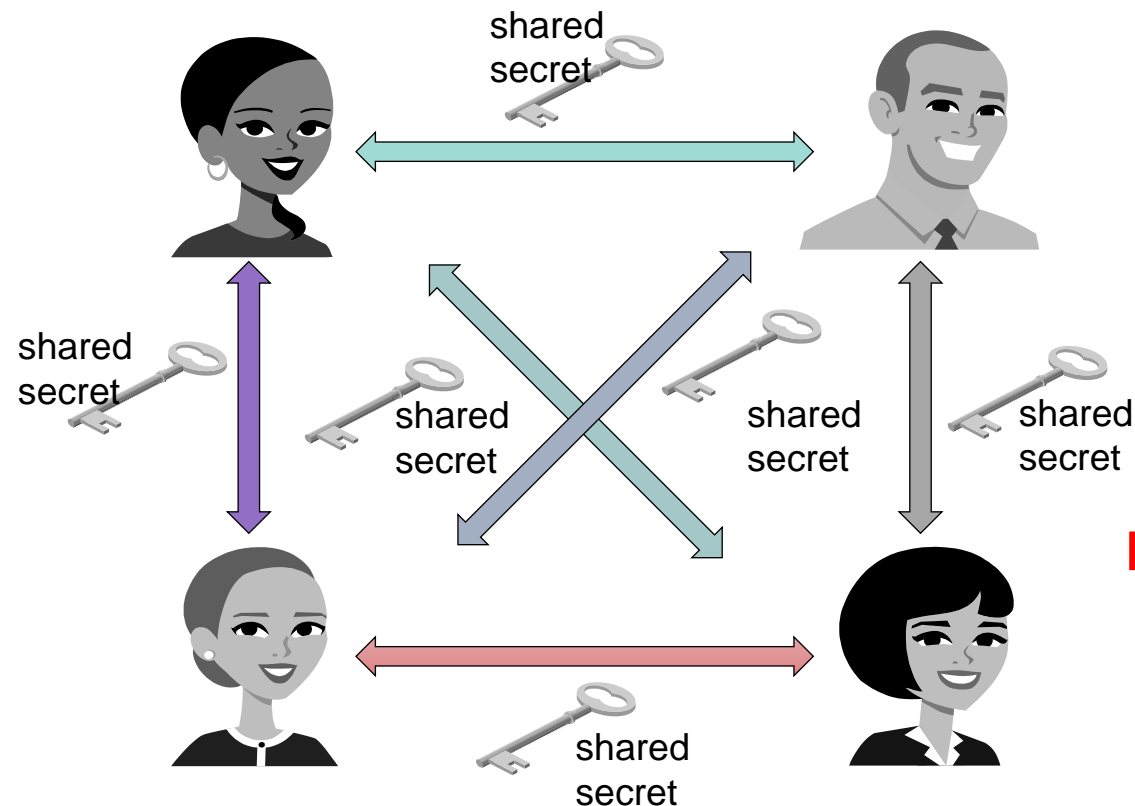
Symmetriske Kryptosystem

- Alice og Bob **deler** en **hemmelig nøkkel** som brukes både til kryptering og dekryptering



Symmetrisk Nøkkel **distribusjon**

- Forutsetter at hvert “par” **deler hver sin** (forskjellige) nøkkel

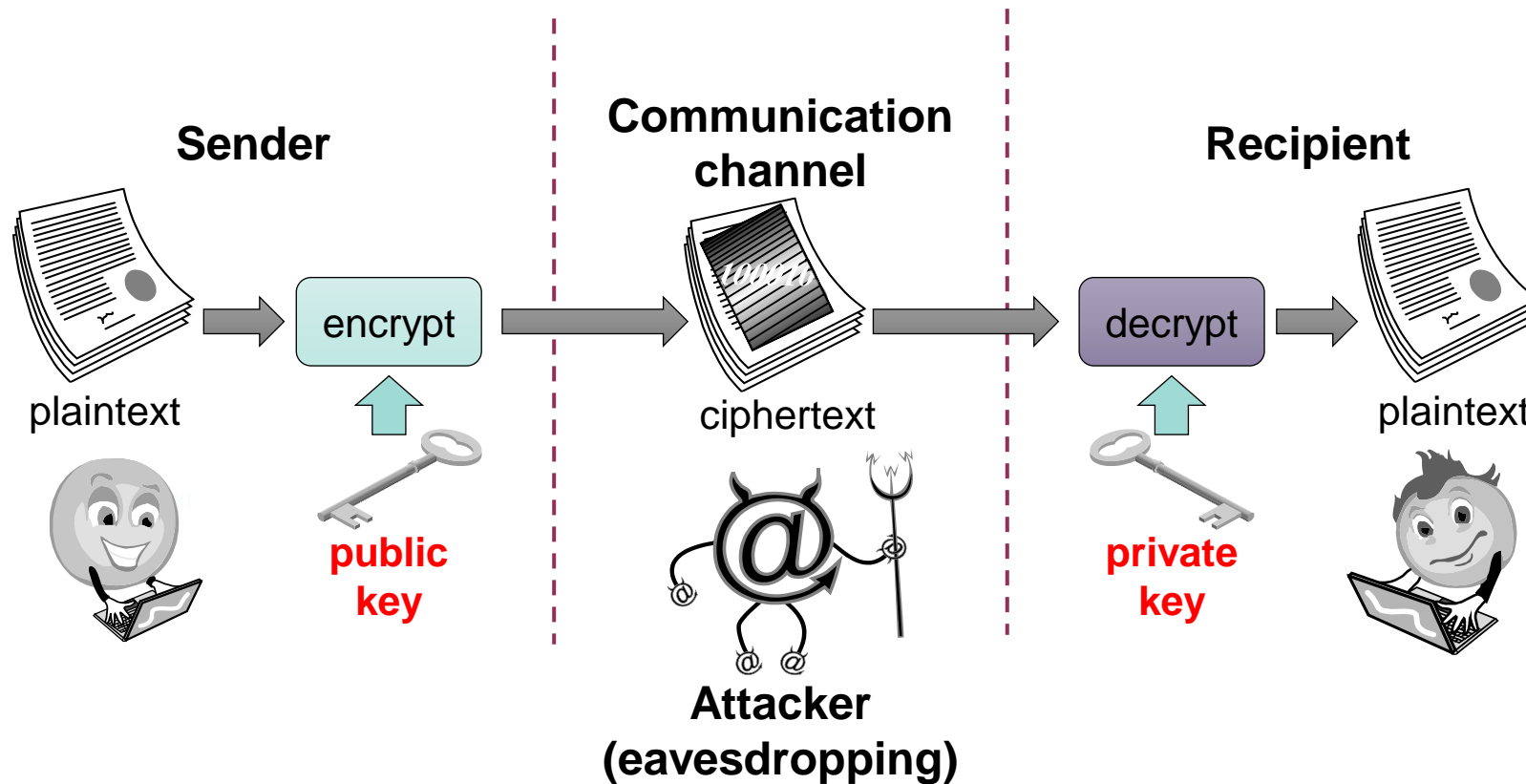


**$n*(n-1)/2$
nøkler**

- Bob har to nøkler:
en **privat nøkkel**, S_B , som Bob holder **hemmelig**, og en
(**offentlig nøkkel**) **public key**, P_B , som Bob **gir til alle**.
 - Når Alice sender en kryptert melding til Bob, så trenger hun bare hans public key, P_B , krypterer meldingen sin M med den, og sender resultatet, $C = E_{P_B}(M)$, til Bob.
Bob kan så bruke sin private nøkkel til å dekryptere meldingen $M = D_{S_B}(C)$.

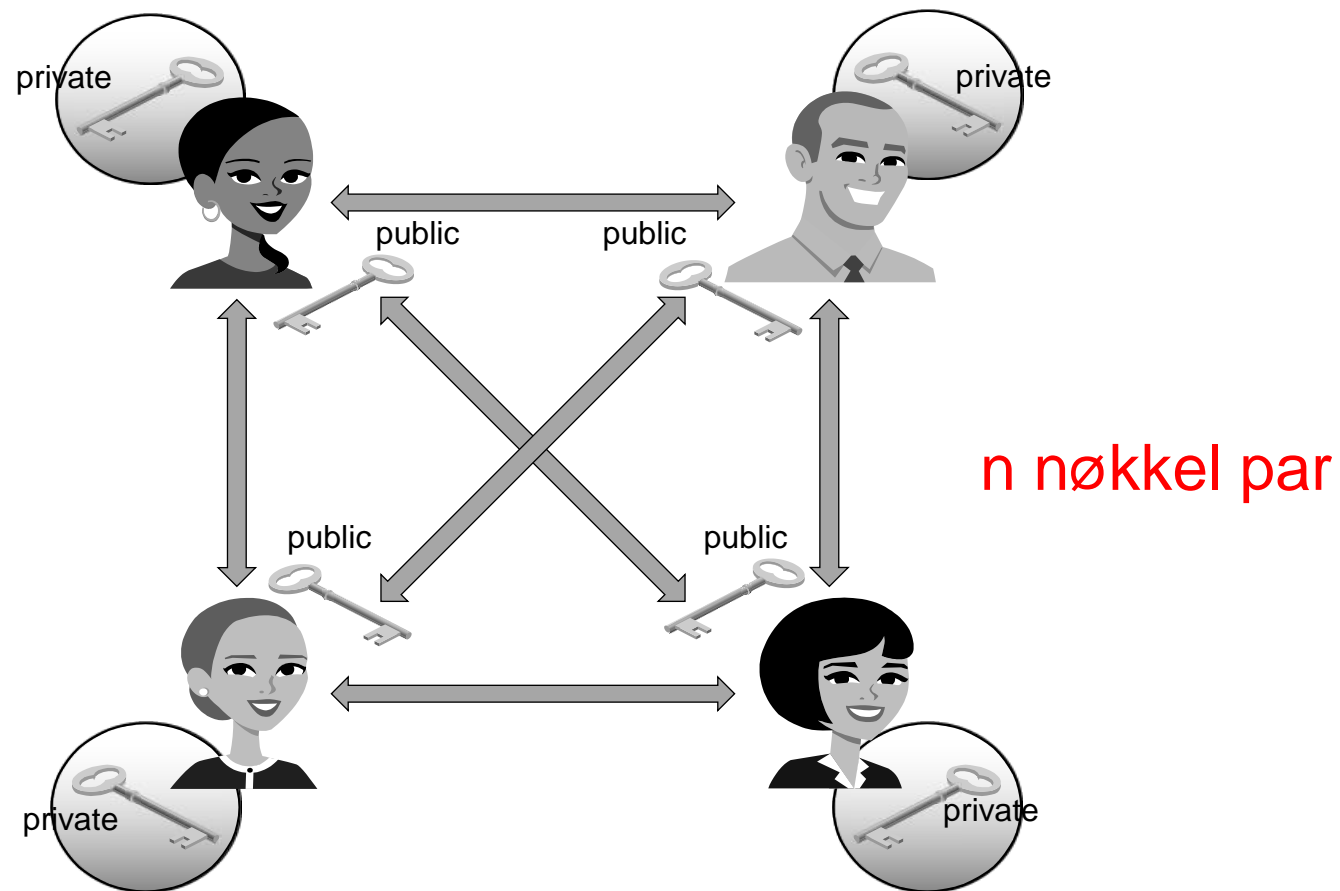
Public-Key Kryptografi

- **Ulike nøkler** brukes for kryptering og dekryptering



Public Key Distribusjon

- Trenger bare en nøkkel pr mottager
- PK-Infrastruktur (**PKI**) er *ikke* dermed lett å få til.



Digital Signatur

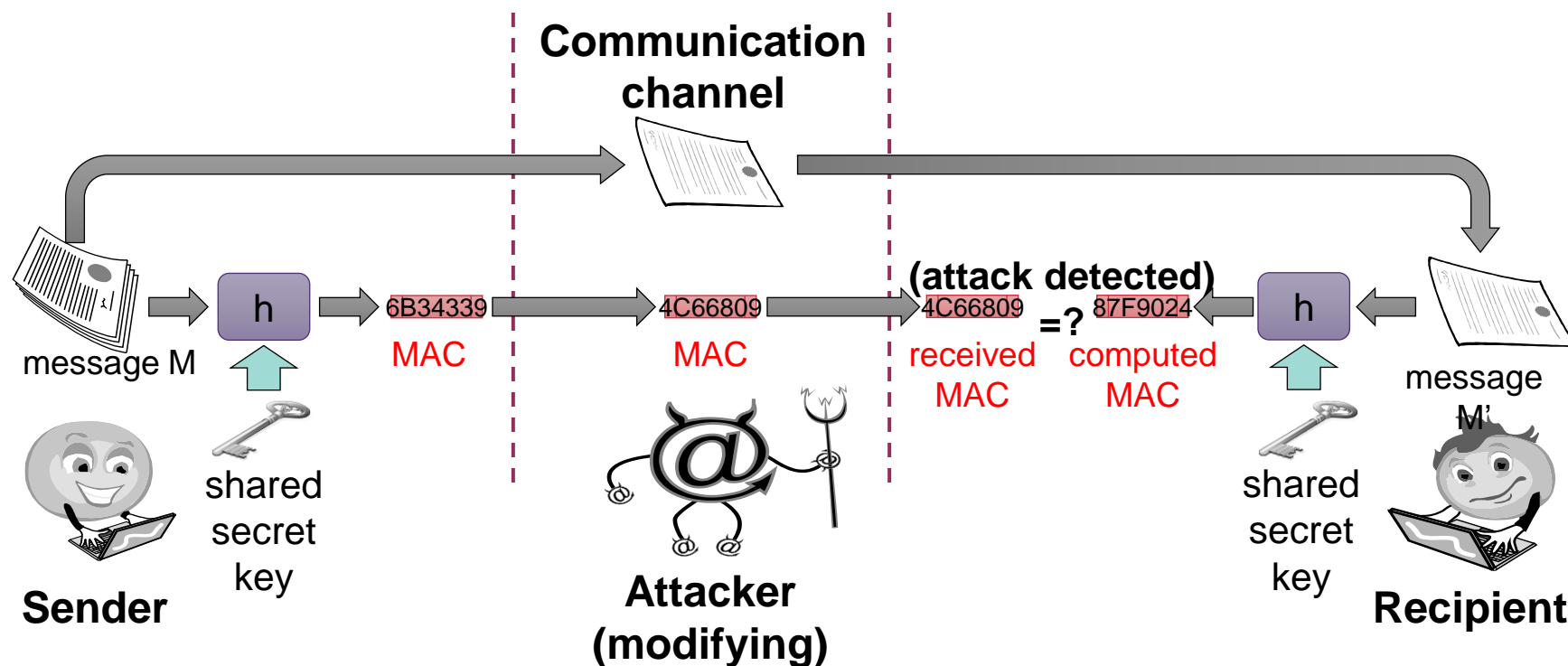
- Public-key kryptering gir en metode for å lage **digitale signaturer**
 - Tilsvarende “underskrift”
- For å signere en melding, M , kryptere bare Alice den med sin **private nøkkel**, S_A , og lager $C = E_{S_A}(M)$.
- Hvem som helst kan dekryptere meldingen med Alice’s **offentlige nøkkel**, og få $M' = D_{P_A}(C)$, som kan sammenlignes med meldingen M .

Kryptografisk Hash Funksjon

- En **sjekksum** på en melding M , som er
- **En-veis**: det skal være lett for computeren å beregne $Y=H(M)$, men svært krevende å finne M når du bare har Y
- **Kollisjon-resistent**: Det skal være vanskelig (usannsynlig) å finne to meldinger, M og N , som er slik at $H(M)=H(N)$.
- **Eksempel**: SHA-1, SHA-256.

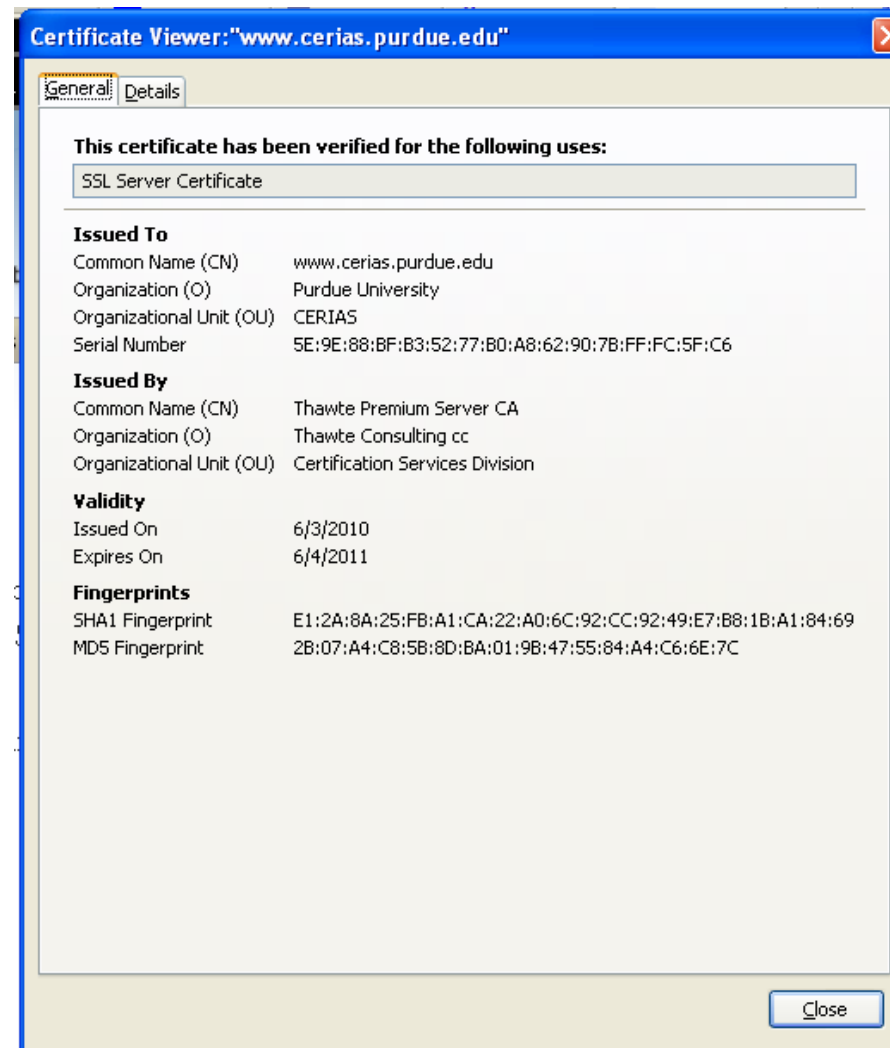
Message Authentication Codes

- Lar Alice og Bob oppnå **data-integritet** når de deler en felles nøkkel
- Gitt meldingen M, beregner Alice $H(K||M)$ og sender M og hash-verdien til Bob.



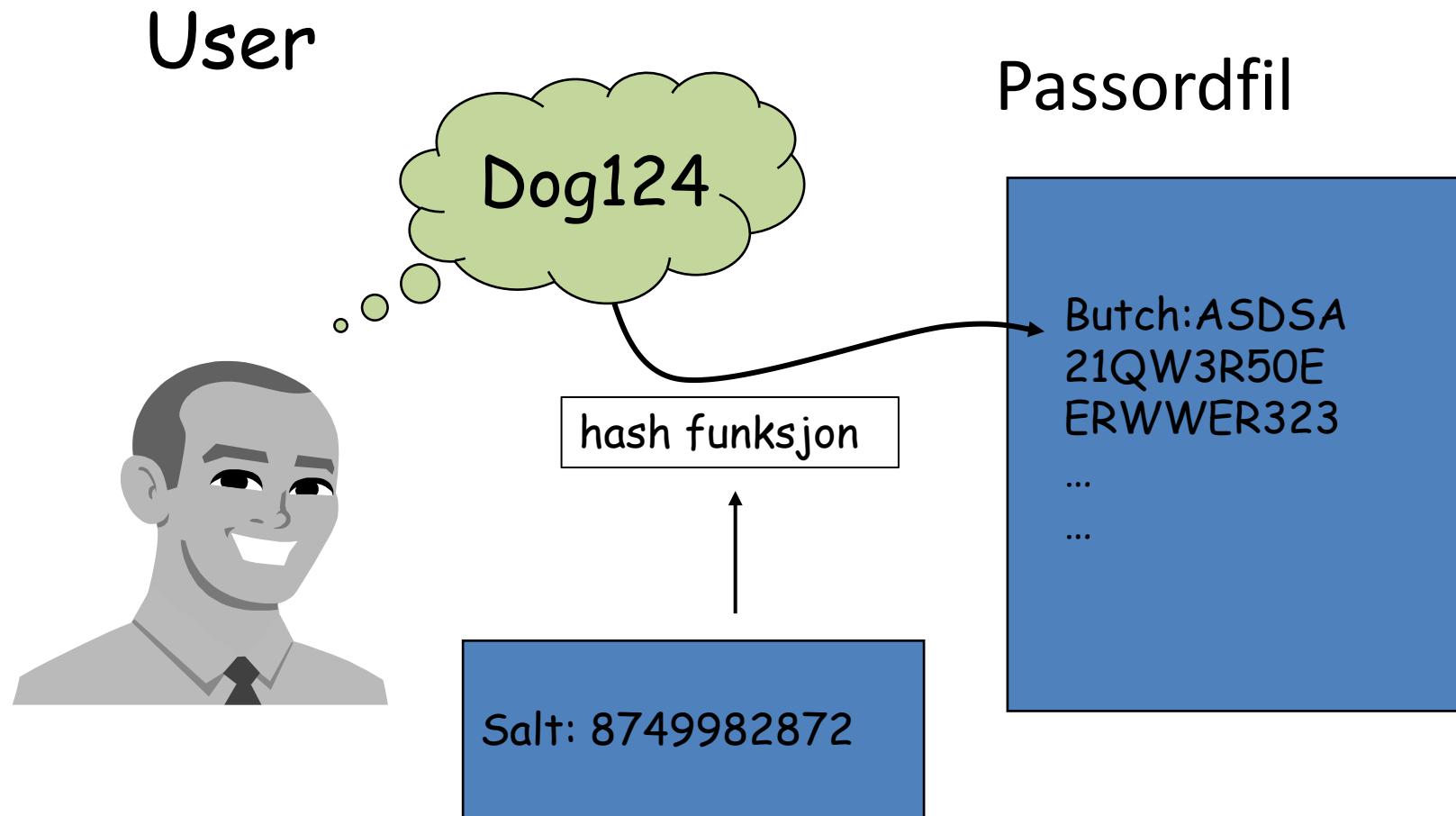
Digitale Sertifikat

- **Certificate Authority (CA)** signerer digitalt sammenhengen mellom en identitet og en offentlig nøkkel som tilhører identiteten



Passord

Hvordan lagres passord?



Passord (som nevnt i TK1104)

- En vanlig måte å måle kvaliteten på et passord er **bitstyrke**
- Uttrykker hvor mange forsøk en tilfeldig angriper **maximalt** trenger for å gjette ("brute force") passordet.
- Bitstyrke = $\lg_2(\text{forskjellige tegn mulige i passorde})^* \text{ antall tegn i passordet}$.
- F.eks. PIN-kode bruker 10 tegn (0-9) og 4 tegn \Rightarrow bitstyrke = $\lg_2(10)^*4 = 3,32*4 = 13,28$
 - NB! Praktisk enhet pga **kombinatorisk eksplosjon**
 - $2^{\text{bitstyrke}} = \text{antall mulige passord som kan lages}$
- Anbefalt bitstyrke i våre dager er ca 80, mao ca tolv bokstaver og tegn!
 - I tillegg bør man selvsagt unngå alt som er knyttet til din egen person, alle vanlige ord (de som finnes i ordbøker) mm

“Sikre passord”

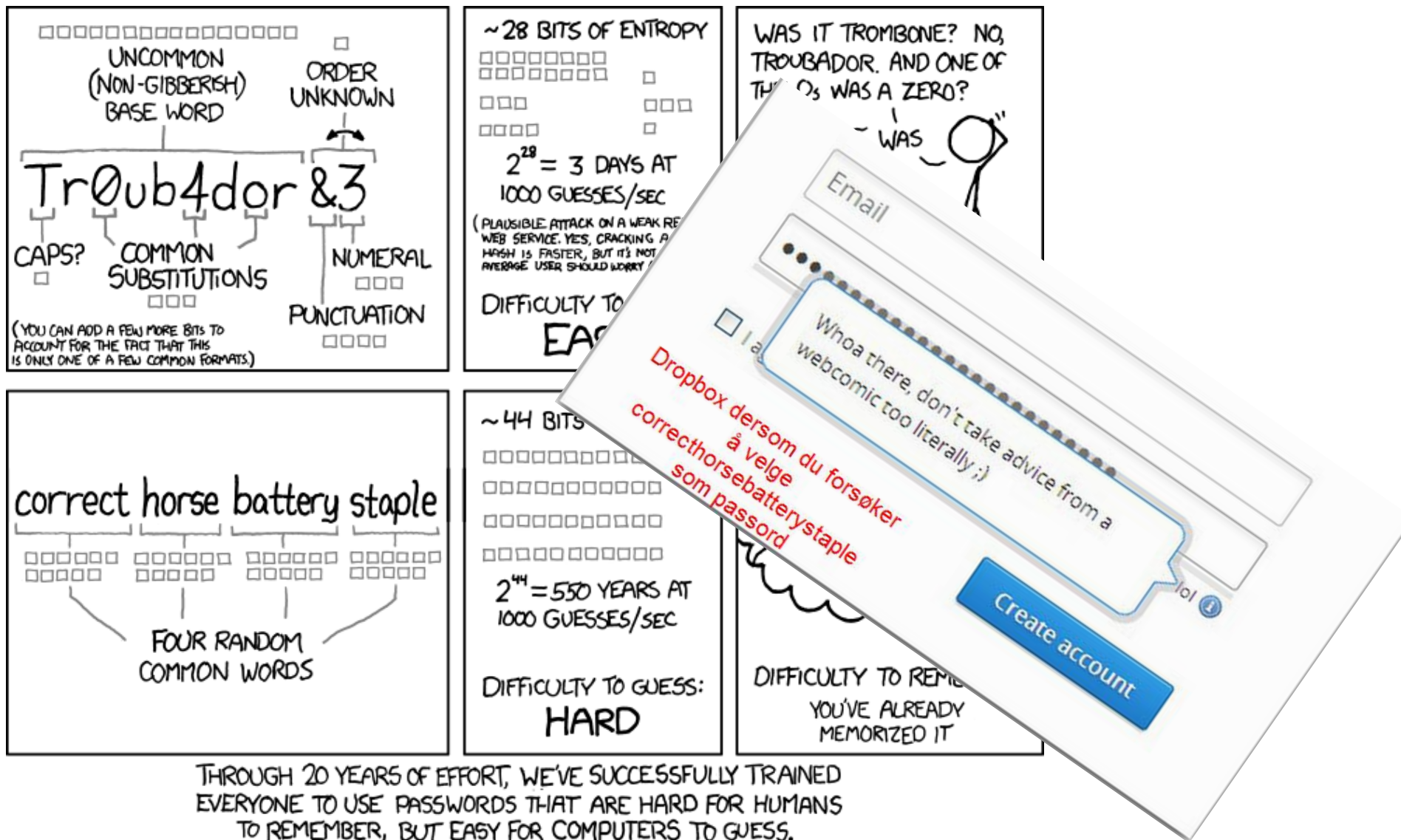
Bør inneholde tegn fra minst tre av gruppene under:

Group	Example
Lowercase letters	a, b, c, ...
Uppercase letters	A, B, C, ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	() ` ~ ! @ # \$ % ^ & * - + = \ { } [] : ; " ' < > , . ? /
Unicode characters	€, Γ, f, and λ

Passfrase er enda bedre: "I re@lly want to buy 11 Dogs!"

Eller lær deg et fint dikt utenatt!!!

XKCD: kommenterer



[illegible]

Passord-safe

- Det finnes mange gode programmer for å oppbevare passord på en sikker måte.
- Ulemper:
- Single point of failure

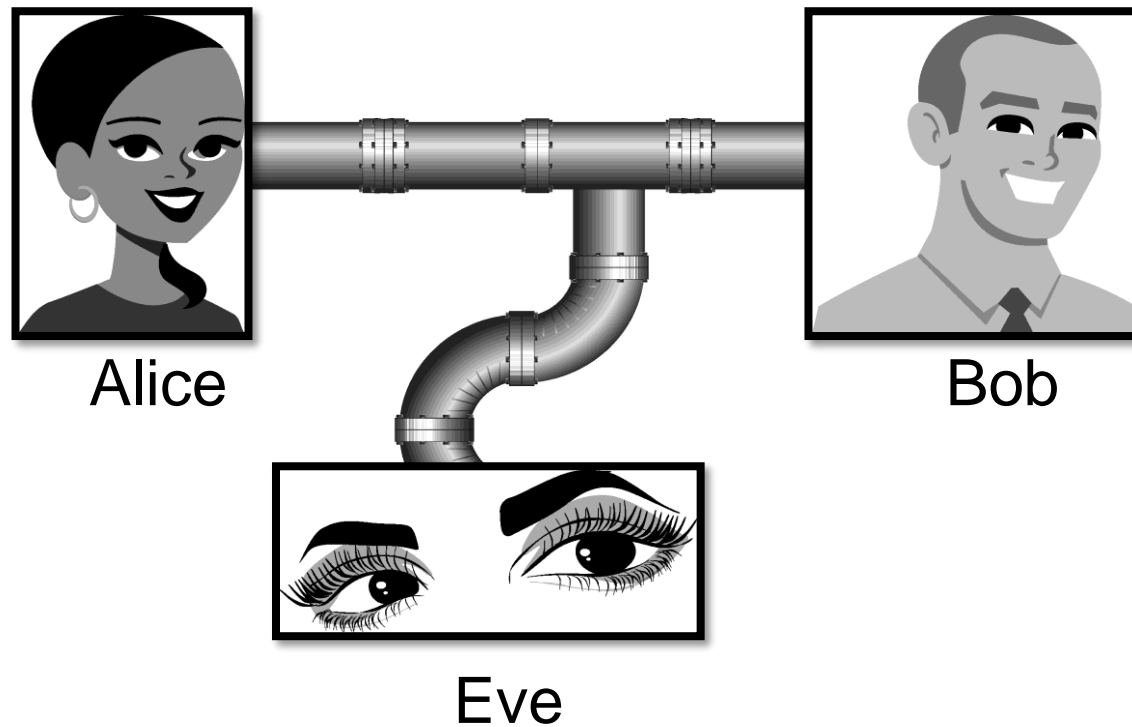


Keepass
Password Safe

Angrep og trusler

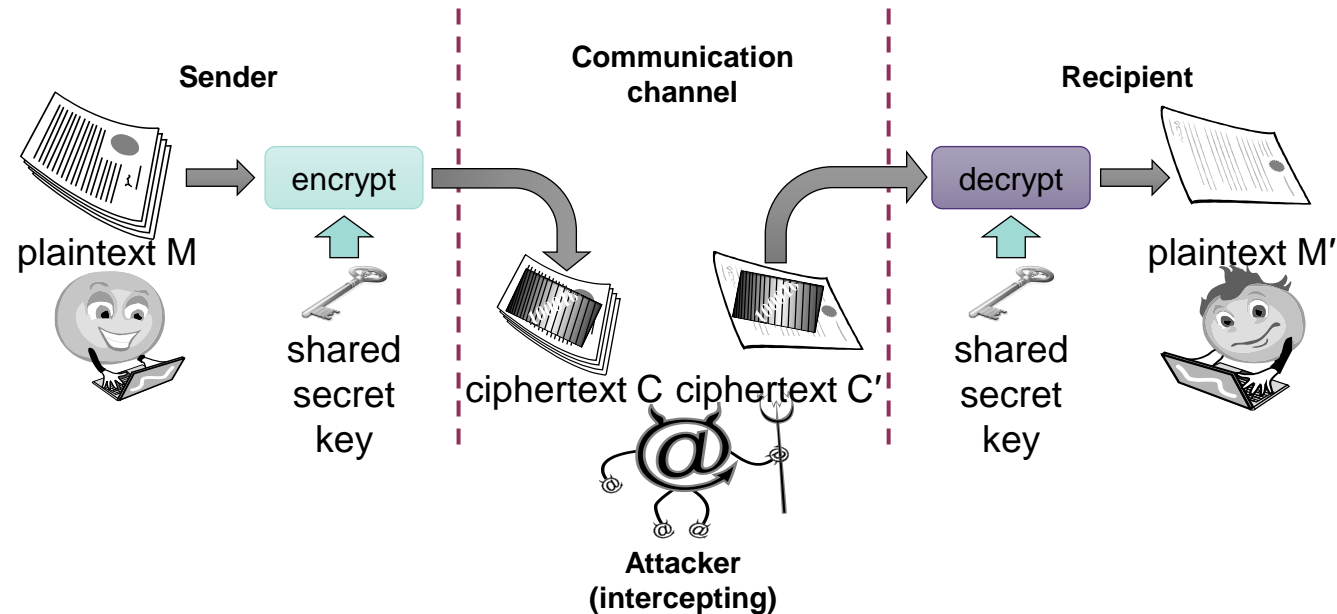
Angrep og trusler

- **Avlytting**: å få tilgang til informasjon som ikke er intendert delt

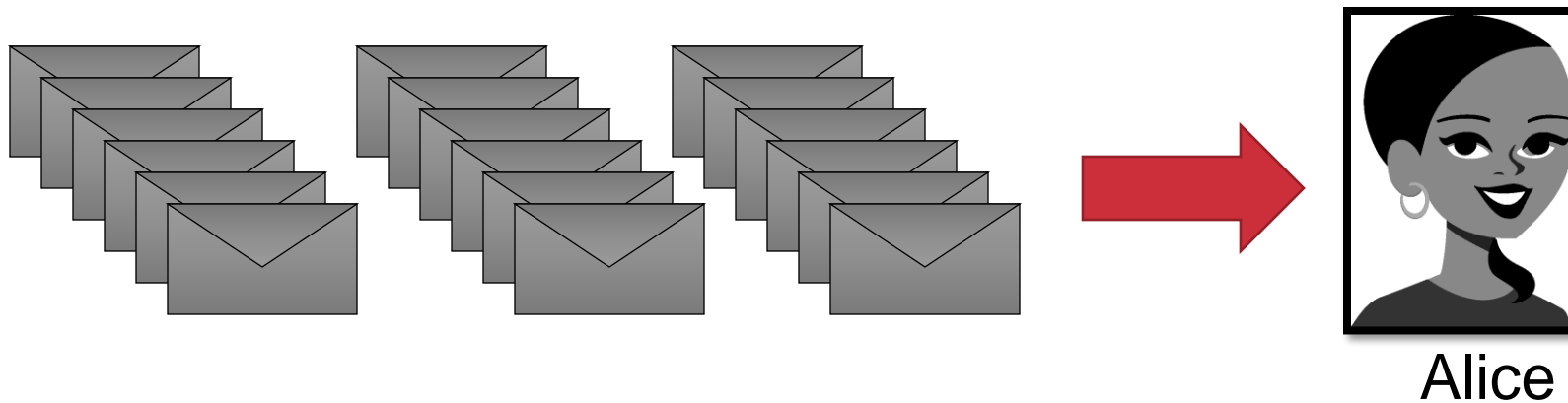


Endring

- **Endring**: uautorisert modifisering av informasjon.
 - **Ex: man-in-the-middle attack**, hvor en datastrøm sendes over et nettverk, overtas ,endres og videresendes.



- **Denial-of-service:** å **avbryte** eller **kraftig forringe** en datatjeneste eller **ødelegge tilgang**
- **Ex:** email **spam**,
 - Angrep på rot-navnetjenerene



- **Masquerading**: å fabrikere informasjon som utgir seg være fra noen som ikke er opphavsmann i virkeligheten.



“From: Alice”
(really is from Eve)

“Social Engineering”

- Innbrudd, bestikkelser og utpressing er vel så effektivt som elektronikk...
- Man kommer ofte like langt, om ikke lenger ved å lure folk, som ved å lure maskinen deres.
- Social Engineering er alle teknikker hvor man lurer mennesker:
 - Ringe noen å utgi seg for å være fra support, banken eller politiet
 - Del ut gratis minnepinner til alle lærere på Høgskolen Kristiania...
 - (Dette er ikke en oppfordring til å angripe lærerne deres!)

Malware, f.eks. Cryptolocker





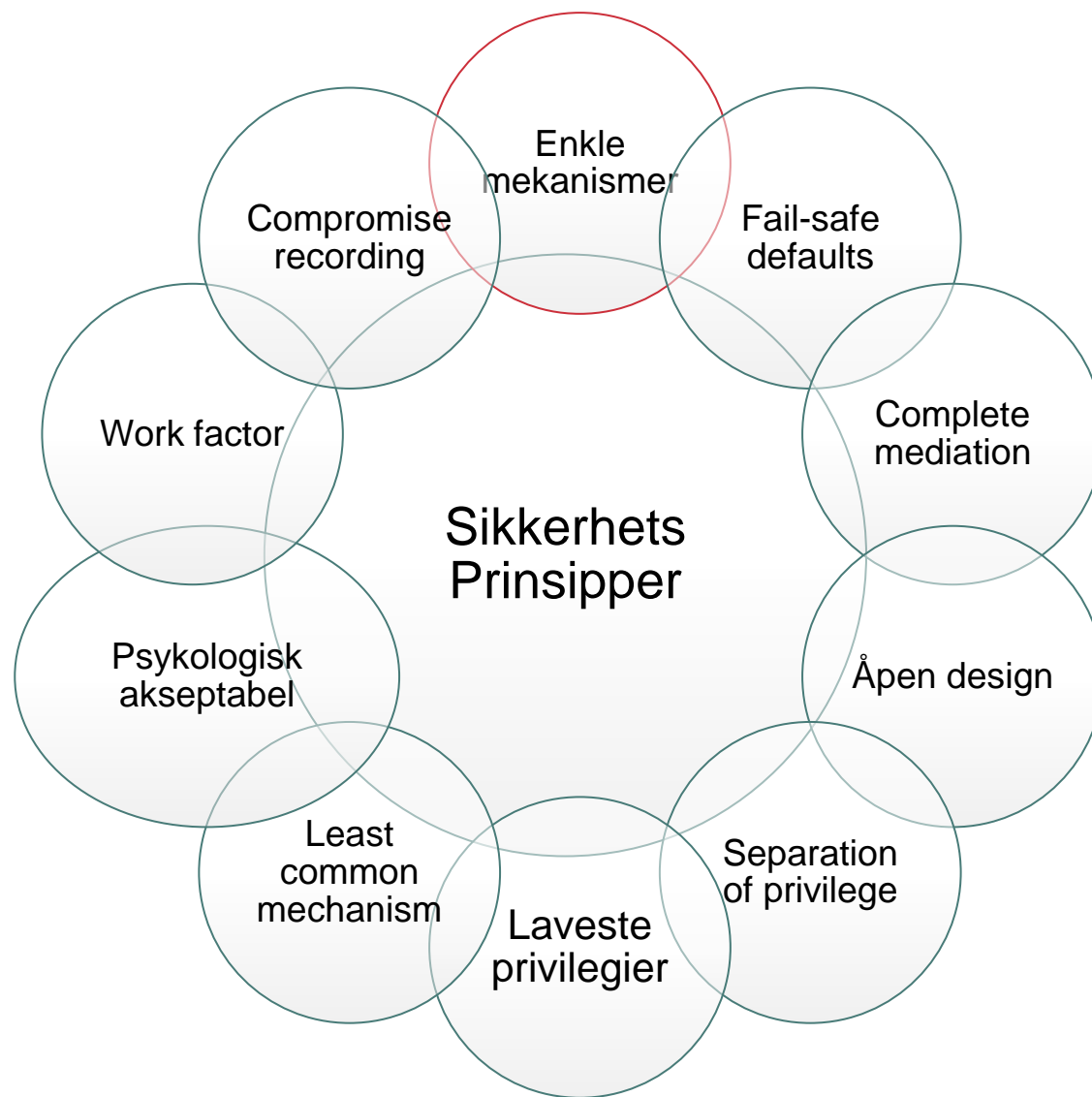
10 prinsipper for sikker design av datasystemer

Disse prinsippene skriver seg fra en klassisk artikkel fra tidlig 70-tall.

Det er ikke meningen å kunne dem på rams

Fokuser på budskapet: Enkelt, åpent, lavest mulig autorisering

De ti sikkerhetsprinsippene



Economy of mechanism



- Så **enkel** mulig **design** og **implementering** av sikkerhets-tiltak
 - Gjelder all programvareutvikling
 - Spesielt viktig i sikkerhetssammenheng fordi
 - Hjelper utviklere og brukere å forstå mål og middel
 - Sikrer effektiv utvikling og verifisering av gjennomføring

Fail-safe defaults



- Standard konfigurering følger et konservativt **beskyttelses-skjema**
 - F.ex. Når du legger til en ny bruker i et operativsystem bør h@n tilhøre en gruppe med minimale adgangsrettigheter til filer og tjenester
 - OS og applikasjoner (f.ex. Browsere) prioriterer ofte “brukervennlighet” over sikkerhet

Complete mediation



- All adgang til en ressurs må sjekkes for om det er i tråd med et beskyttelses-skjema
 - Bør være skeptisk til å mellomlagre (“cache”) autoriseringer (tokens) av ytelseshensyn siden rettigheter kan endre seg over tid
 - F.ex. bør en nettbank kreve ny pålogging etter f.eks. 15 minutter.

Open design



- Arkitektur og design bør være offentlig tilgjengelig
 - Sikkerhet bør baseres på at bare kryptografiske nøkler er hemmelige
 - Åpen design tillater at systemet kan undersøkes av mange forskjellige parter som vil lede til raskere oppdagelse og retting av sårbarheter som skyldes design-feil.
 - Dette er det motsatte av “**security by obscurity**”, hvor man forsøker å hemmeligholde f.eks. kryptografiske algoritmer (hvilket historisk sette aldri har fungert...)

Separation of privilege



- Flere ulike betingelser bør/må kreves innfridd for å få tilgang til ressurser eller at et program skal utføre en bestemt handling.
- Systemet bør være modularisert på en slik måte at kompromitering av en komponent ikke sprer seg til hele.

Least privilege



- Hvert program bør operere med kun det **minimum av rettigheter** det trenger for å fungere skikkelig.
 - Tilsvarende det militære **need-to-know** prinsippet for informasjonsdeling.
 - Dersom man følger prinsippet er muligheten til å misbruke rettigheter begrenset, og skaden som kan oppstå ved at en bestemt bruker-konto eller applikasjon blir kompromitert er minst mulige.

Least common mechanism



- I systemer med flere brukere bør mekanismer som tillater deling av en ressurs mellom flere brukere minimeres.
 - F.ex. Dersom mer enn en bruker trenger tilgang til en fil eller applikasjon så bør disse få tilgang gjennom ulike kanaler for å forhindre uforutsette konsekvenser som kan medføre sikkerhetsproblemer.

Psychological acceptability



- Bruker-grensesnitt og tilbakemeldinger bør være godt designet og “intuitive” og alle sikkerhets-innstillinger bør være i tråd med hva en “vanlig bruker” forventer.



- **Kostnaden ved å omgå/bryte** en sikkerhets-mekanisme bør sammenlignes med de ressursene en forventet angriper vil disponere, når man designer et sikkerhetskjema
 - Et system som skal beskytte karakterene til studentene i en database, hvor studenter og snokere er typiske angripere; trenger sannsynligvis ikke å være like sofistikert/avansert som et system som skal beskytte atomvåpen eller industrihemmeligheter.

Compromise recording



- Noen ganger er det bedre å få oversikt (loggføre) konsekvensene av et inngrep enn å sette inn mer sofistikerte tiltak for å forhindre det.
 - Overvåkningskamera kan være å foretrekke fremfor å sikre alle dører og vinduer bedre.
 - Serverene i et nettverk kan logge all fil-adgang, alle eposter sendt og mottatt og all browsing-sesjoner.
 - (Mest aktuelt for fysisk sikring, mindre for software – der er dog logging uansett viktig! Bl.a. for å kunne anmelde!)

fin



Hva skal vi kunne?

- Definere «informasjonssikkerhet» ut fra C.I.A.
 - Forklare hva konfidensialitet, integritet, tilgjengelighet er og betyr.
- Sikkerhet og trusselbilde
- Resten kommer vi tilbake til gjennom semesteret...

Dagens øving

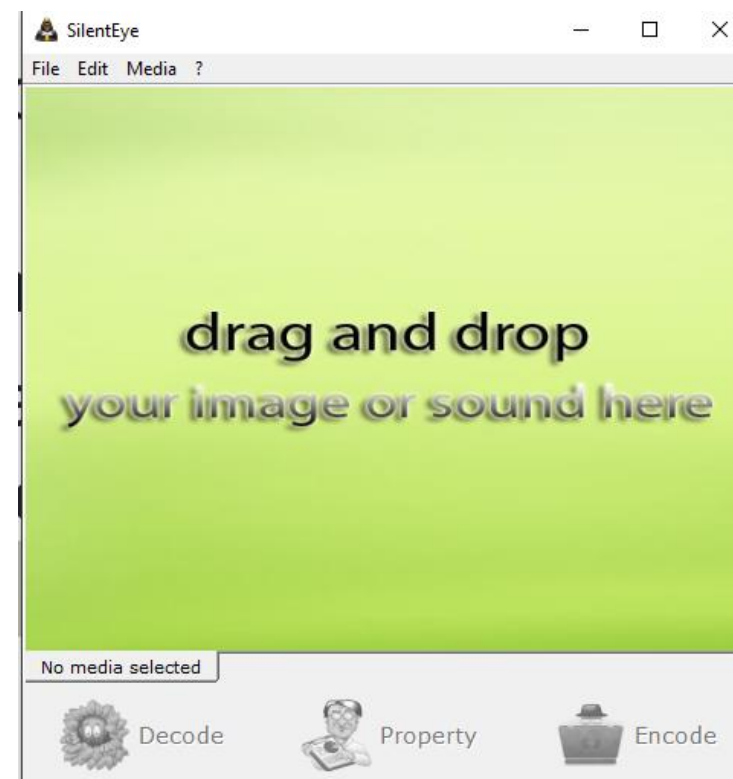
Først en tekst-oppgavesett om C.I.A

Så...

Steganografi



- Skal se nærmere på en teknikk for å kryptere og gjemme filer/meldinger inne i andre filer/meldinger på en (tilnærmet) usynlig måte.
- Kan være litt tidkrevende, med burde være opplysende og «gøyalt» -- men ikke alt for nyttig, håper jeg..
- Tenk gjennom hva det kan brukes til...



(Støttes ikke på 64-bit eller ARM OSX)

<https://achorein.github.io/silenteeye/download/?i2>



- Mange lærer seg sikkerhet og computer science generelt gjennom «capture the flag» (CTF) øvelser
- Steganografi er populært på slike utfordringer
- God ressurs å sjekke ut hvis man skal prøve på CTF:
- <https://0xrick.github.io/lists/stego/>

Øvingsoppgaver?

- TK2100_F00_øvingsoppgaver.pdf i Canvas