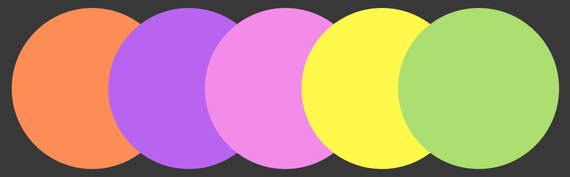
Ånund Kielland Jore

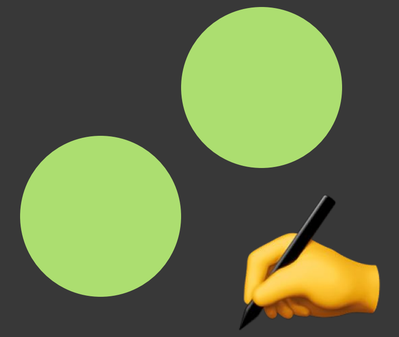
Onsdag 16 Oktober

Kryptografi og lagdeling



IN1020

1. Diskutere noen oppgaver
2. Pause
3. Diskutere noen eksamensoppgaver
4. Selvstendig arbeid





Ukens Serietips - Devs

- “A computer engineer investigates the secretive development division in her company, which she believes is behind the disappearance of her boyfriend”

Hva har jeg gjort siden sist?

Jeg har nå fått tilbud om Software Engineer internship hos....

Videre til faglige ting

Noen definisjoner

- IP-adresse: Skiller bare mellom adresser innenfor og utenfor det lokale nettverket (LAN)
- LAN: Local Area Network, dekker vanligvis et lite område, typisk et enkelt bygg eller en gruppe bygninger i nærhet til hverandre
- Subnett: forhindre at IP-adresser sløses bort
- Broadcast: Levere til alle enheter som er koblet på samme LAN (nettverk)
- Gateway: nødvendig når man kobler sammen nettverk som bruker ulike kommunikasjonsprotokoller

Mini repetisjon fra sist: IP-konvertering

20 **Punktnotasjon til CIDR**

En datamaskin har IP-adressen 192.168.100.14
Nettverksmasken er: 255.255.255.248
Hva er IP-adressen til maskinen i CIDR-notasjon?

Man konverterer nettverksmasken til binært og sjekker hvor stor del er tildelt nettverket

255.255.255.248

||

11111111.11111111.11111111.11111000

Man har totalt 32 bit (8x4), 3 er tildelt vertsdel, resten er til nettverksdel

32-3=29

CIDR-notasjon: 192.168.100.14/29

3(b) Subnet - Kringkastingsadresse

En gyldig IP-adresse på et subnett er 134.1.98.45. Nettverksmasken til subnettet er 255.255.248.0 Hva er kringkastingsadressen til dette subnettet?

Husk OR operasjon når man konverterer til kringkastningsadresse og bruk den inverse nettverksmasken

A	B	F
0	0	0
0	1	1
1	0	1
1	1	1

134.1.98.45
10000110.00000001.01100010.00101101

255.255.248.0
11111111.11111111.11111000.00000000

3(b) Subnet - Kringkastingsadresse

En gyldig IP-adresse på et subnett er 134.1.98.45. Nettverksmasken til subnettet er 255.255.248.0 Hva er kringkastingsadressen til dette subnettet?

Husk OR operasjon når man konverterer til kringkastningsadresse og bruk den inverse nettverksmasken

A	B	F
0	0	0
0	1	1
1	0	1
1	1	1

134.1.98.45
10000110.00000001.01100010.00101101

255.255.248.0
11111111.11111111.11111000.00000000

0000000.0000000.00000111.11111111 (invers)
OR
10000110.00000001.01100001.00101101
||

3(b) Subnet - Kringkastingsadresse

En gyldig IP-adresse på et subnett er 134.1.98.45. Nettverksmasken til subnettet er 255.255.248.0 Hva er kringkastingsadressen til dette subnettet?

Husk OR operasjon når man konverterer til kringkastningsadresse og bruk den inverse nettverksmasken

A	B	F
0	0	0
0	1	1
1	0	1
1	1	1

134.1.98.45
10000110.00000001.01100010.00101101

255.255.248.0
11111111.11111111.11111000.00000000

0000000.0000000.00000111.11111111 (invers)
OR
10000110.00000001.01100001.00101101
||
10000110.00000001.01100111.11111111

Broadcast: 134.1.103.255

IP-adresse, finn subnettsadressen

IP-adresse: 192.168.1.5/24
Konverter til subnettsadressen

Husk AND operasjon når man konverterer til subnettsadresse

192.168.1.5
11000000.10101000.00000001.00000101

AND

A	B	F
0	0	0
0	1	0
1	0	0
1	1	1

IP-adresse, finn subnettsadressen

IP-adresse: 192.168.1.5/24
Konverter til subnettsadressen

Husk AND operasjon når man konverterer til subnettsadresse

A	B	F
0	0	0
0	1	0
1	0	0
1	1	1

192.168.1.5
11000000.10101000.00000001.00000101

AND

11111111.11111111.11111111.00000000 (24)

IP-adresse, finn subnettsadressen

IP-adresse: 192.168.1.5/24
Konverter til subnettsadressen

Husk AND operasjon når man konverterer til subnettsadresse

A	B	F
0	0	0
0	1	0
1	0	0
1	1	1

192.168.1.5
11000000.10101000.00000001.00000101

AND

11111111.11111111.11111111.00000000 (24)

||

11000000.10101000.00000001.00000000

Subnettsadresse: 192.168.1.0

DHCP (Dynamic Host Configuration Protocol)

- Automatisk utdeling av IP-adresser
  - Eliminerer behovet for manuell konfigurering på hver enhet
- **Discover ->**
  - DHCP-klienten sender en DHCP Discover-melding som sendes som broadcast for å finne DHCP-servere på nettverket (til f.eks. en ruter)
- **Offer ->**
  - DHCP-serveren som mottar forespørselen, svarer med en DHCP Offer-melding som inneholder et tilbud med IP-adresse, subnettmaske, gateway mm
- **Request ->**
  - DHCP-klienten sender en DHCP Request-melding for å signalisere at den godtar tilbudet
- **Acknowledgment ->**
  - DHCP-serveren bekrefter tildelingen med en DHCP Acknowledgment (ACK)-melding

ARP - koblingen mellom nettverkslaget og linklaget

- Nettverkslaget:
  - IP-adresser
- Linklaget:
  - MAC-adresser
- En enhet vil snakke med en annen enhet på samme nettverk
  - Den har den private IP adressen til mottakeren - men ikke MAC-adressen
  - Hvordan får den MAC-adressen?
- ARP-cache
  - arp -a / arp -ne

ARP - koblingen mellom nettverkslaget og linklaget

- Nettverkslaget:
  - IP-adresser
- Linklaget:
  - MAC-adresser
- En enhet vil snakke med en annen enhet på samme nettverk
  - Den har den private IP adressen til mottakeren - men ikke MAC-adressen
  - Hvordan får den MAC-adressen?
- ARP-cache
  - arp -a / arp -ne

ARP - oppgaver



15 **ARP**

Protokollen "ARP" brukes til å:
Velg ett eller flere alternativer

Sikre at datapakker ikke går i evig løkke i nettverket.

Koble sammen adresser i "Nettverkslaget" med adresser i "Linklaget".

Oversette domenenavn til IP-adresser.

Dele ut IP-adresser til maskiner som kobler på nettverket.

3(c) **ARP-tabell**

Hva er en ARP-tabell?
Velg ett alternativ

En liste over IP-adresser og portnummer brukt for å gjøre det mulig for private adresser på et subnett å koble seg opp mot andre maskiner på Internett (utenfor eget LAN)

En liste over mulige ruter som en IP-pakke kan ta gjennom Internett.

En liste, vedlikeholdt av en vert på et subnett, med IP-adresser og MAC-adresser til andre verter på samme subnett.

En tabell som viser når forskjellige ARP-pakker er klare til å sendes ut.

ARP - oppgaver



15 ARP

Protokollen "ARP" brukes til å:
Velg ett eller flere alternativer

- [ ] Sikre at datapakker ikke går i evig løkke i nettverket.
- [x] Koble sammen adresser i "Nettverkslaget" med adresser i "Linklaget".
- [ ] Oversette domenenavn til IP-adresser.
- [ ] Dele ut IP-adresser til maskiner som kobler på nettverket.

3(c) ARP-tabell

Hva er en ARP-tabell?
Velg ett alternativ

- En liste over IP-adresser og portnummer brukt for å gjøre det mulig for private adresser på et subnett å koble seg opp mot andre maskiner på Internett (utenfor eget LAN)
- En liste over mulige ruter som en IP-pakke kan ta gjennom Internett.
- En liste, vedlikeholdt av en vert på et subnett, med IP-adresser og MAC-adresser til andre verter på samme subnett.
- En tabell som viser når forskjellige ARP-pakker er klare til å sendes ut.

ARP - oppgaver



15 ARP

Protokollen "ARP" brukes til å:
Velg ett eller flere alternativer

- [ ] Sikre at datapakker ikke går i evig løkke i nettverket.
- [x] Koble sammen adresser i "Nettverkslaget" med adresser i "Linklaget".
- [ ] Oversette domenenavn til IP-adresser.
- [ ] Dele ut IP-adresser til maskiner som kobler på nettverket.

3(c) ARP-tabell

Hva er en ARP-tabell?
Velg ett alternativ

- ( ) En liste over IP-adresser og portnummer brukt for å gjøre det mulig for private adresser på et subnett å koble seg opp mot andre maskiner på Internett (utenfor eget LAN)
- ( ) En liste over mulige ruter som en IP-pakke kan ta gjennom Internett.
- (x) En liste, vedlikeholdt av en vert på et subnett, med IP-adresser og MAC-adresser til andre verter på samme subnett.
- ( ) En tabell som viser når forskjellige ARP-pakker er klare til å sendes ut.

Ruteren sin oppgave i nettet

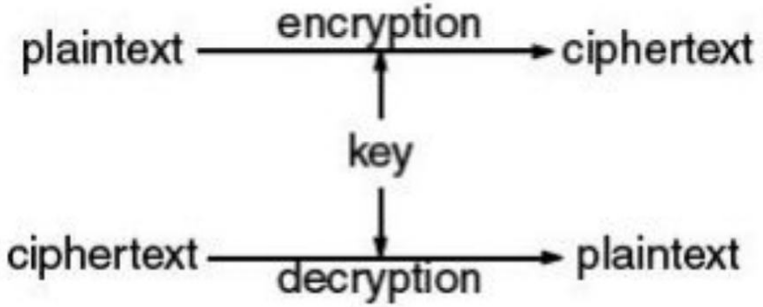
- **Ruting:** videresending av datapakker
- **Internet Service Provider (ISP):** driver et nettverk
- **ISP Peering:** ISPer avtaler med hverandre om å videresende til og fra hverandre
- **Border Gateway Protocol:** Rutingprotokoll
- **OSPF:** eksempel på rutingalgoritme for mindre nettverk

Mini-mini-mini repetisjon av viktige begreper som er lette å misforstå, blande sammen, eller rett og slett bare glemme, noe som er dumt siden de sikkert kommer på eksamen

- TCP vs UDP
  - **TCP:** Tilkoblingsorientert, handshake, ack, levering i riktig rekkefølge, pålitelig
  - **UDP:** Forbindelsesløs, ikke pålitelig, ikke nødvendigvis riktig rekkefølge, send-og-håp, rask
- Metningskontroll vs flytkontroll
  - **Metningskontroll:** Passer på at nettverket ikke blir overbelastet. Mottaker kan potensielt motta raskere enn nettverket har kapasitet til.
  - **Flytkontroll:** Sjekker hvor fort mottaker kan motta, sender ikke raskere enn dette

Symmetrisk kryptering

- Består av **én nøkkel** som brukes til å kryptere og dekryptere fra og til mellom plain text og chipher text.
- **Nøkkelen må være hemmelig**, kun kjent av rettmessige aktører, ellers kan alle dekryptere meldingen.
- Men hvordan utveksle nøkkel på sikker måte? For å gjøre det trenger man asymmetrisk kryptering



Fra eksamen 2022

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Usant	Sant
Kan brukes for å sikre uavviselighet.		
Benyttes til såkalt digital signatur.		
Kan brukes for å sikre konfidensialitet for data.		
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.		
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres		
Benyttes til kryptering av hemmelige meldinger.		
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.		
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.		

Fra eksamen 2022

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

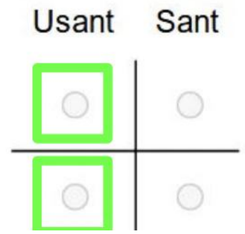
Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Usant	Sant
Kan brukes for å sikre uavviselighet.	○	○
Benyttes til såkalt digital signatur.		
Kan brukes for å sikre konfidensialitet for data.		
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.		
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres		
Benyttes til kryptering av hemmelige meldinger.		
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.		
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.		

Fra eksamen 2022

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?



Kan brukes for å sikre uavviselighet.

Benyttes til såkalt digital signatur.

Kan brukes for å sikre konfidensialitet for data.

Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.

Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres

Benyttes til kryptering av hemmelige meldinger.

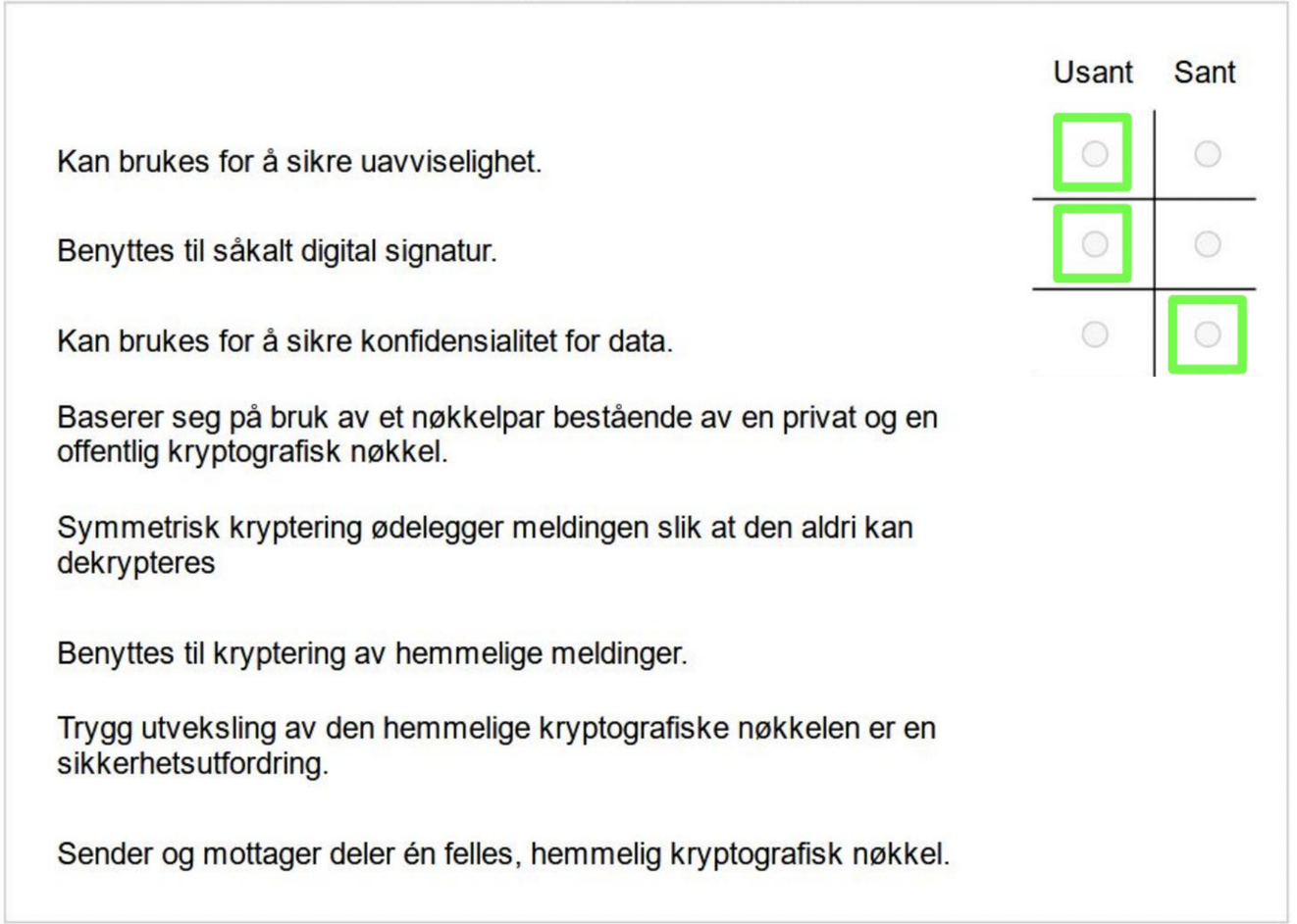
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.

Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.

Fra eksamen 2022

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

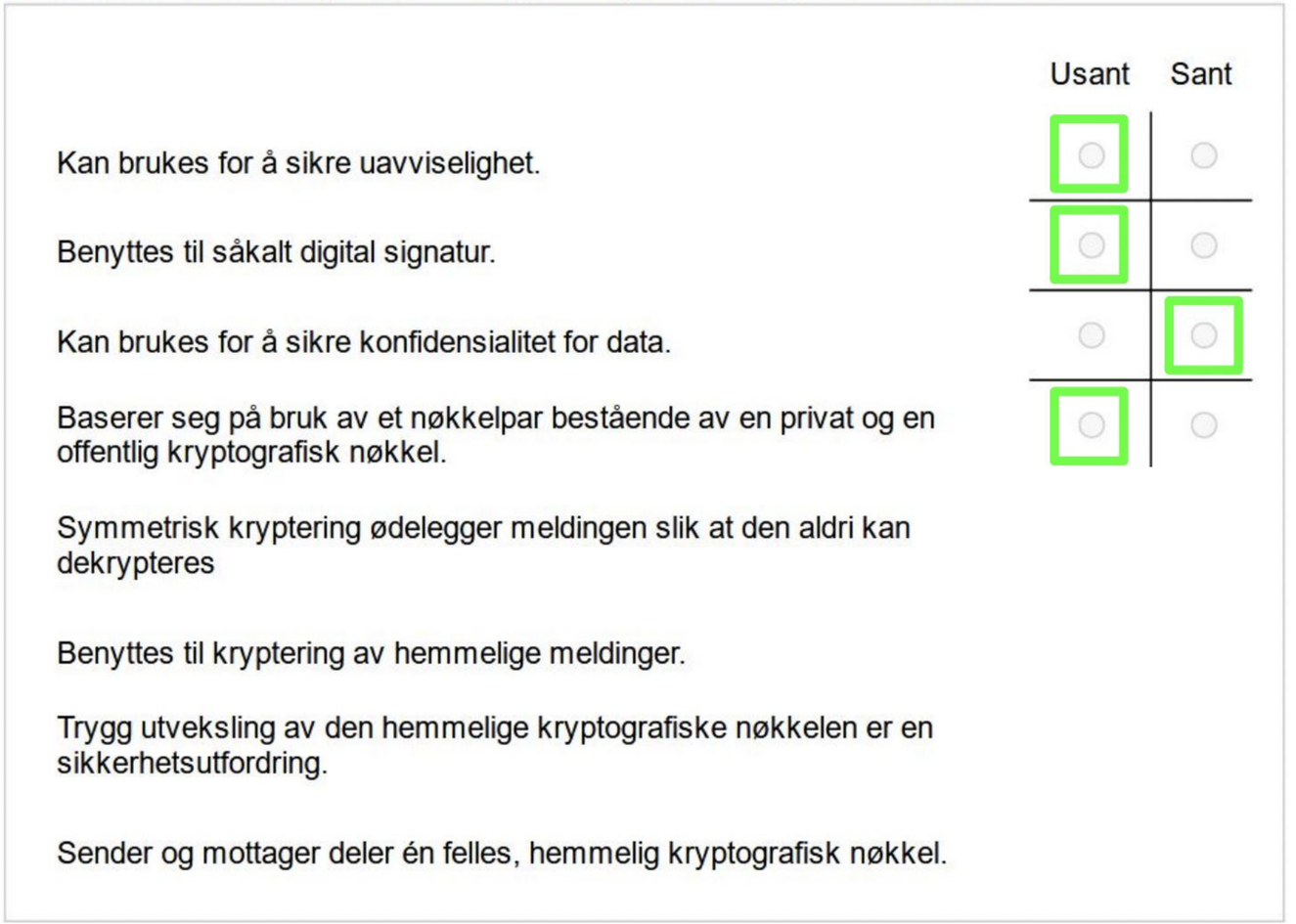
Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?



Fra eksamen 2022

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?



	Usant	Sant
Kan brukes for å sikre uavviselighet.	○	○
Benyttes til såkalt digital signatur.	○	○
Kan brukes for å sikre konfidensialitet for data.	○	○
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.	○	○
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres		
Benyttes til kryptering av hemmelige meldinger.		
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.		
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.		

Fra eksamen 2022

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Usant	Sant
Kan brukes for å sikre uavviselighet.	○	○
Benyttes til såkalt digital signatur.	○	○
Kan brukes for å sikre konfidensialitet for data.	○	○
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.	○	○
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres	○	○

Benyttes til kryptering av hemmelige meldinger.

Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.

Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.

Fra eksamen 2022

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Usant	Sant
Kan brukes for å sikre uavviselighet.	○	○
Benyttes til såkalt digital signatur.	○	○
Kan brukes for å sikre konfidensialitet for data.	○	○
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.	○	○
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres	○	○
Benyttes til kryptering av hemmelige meldinger.	○	○
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.		
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.		

Fra eksamen 2022

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Usant	Sant
Kan brukes for å sikre uavviselighet.	○	○
Benyttes til såkalt digital signatur.	○	○
Kan brukes for å sikre konfidensialitet for data.	○	○
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.	○	○
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres	○	○
Benyttes til kryptering av hemmelige meldinger.	○	○
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.	○	○
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.		

Fra eksamen 2022

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Usant	Sant
Kan brukes for å sikre uavviselighet.	○	○
Benyttes til såkalt digital signatur.	○	○
Kan brukes for å sikre konfidensialitet for data.	○	○
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.	○	○
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres	○	○
Benyttes til kryptering av hemmelige meldinger.	○	○
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.	○	○
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.	○	○

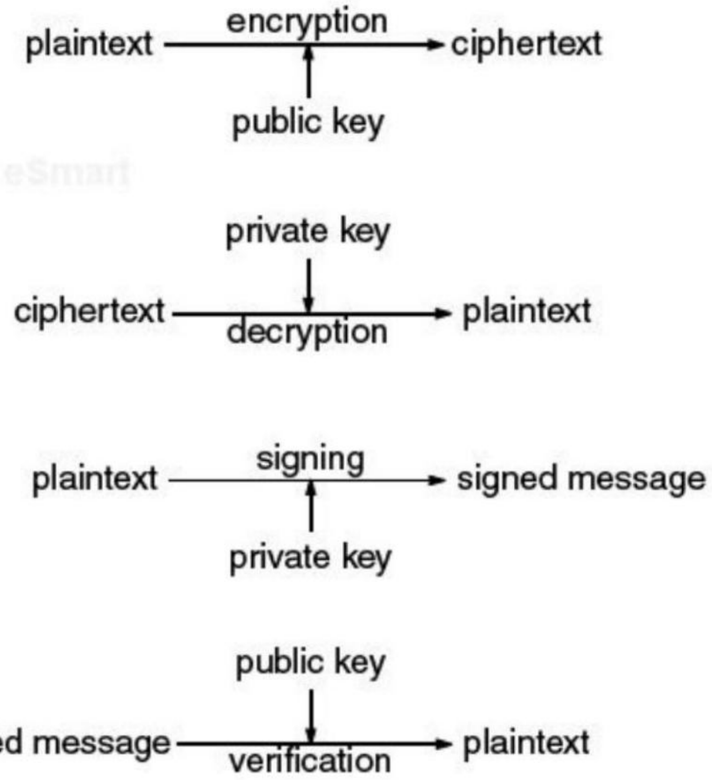
Asymmetrisk kryptering

Vi har her **to ulike nøkler. Den ene er offentlig og den andre er hemmelig**.

1. Dersom du bruker asymmetrisk kryptering for å kryptere meldinger (konfidensialitet) er det offentlig nøkkel som brukes til kryptering, mens privat nøkkel brukes til å dekryptere.

2. Dersom du bruker asymmetrisk kryptering til digital signatur (autentisering) brukes privat nøkkel til å kryptere, mens offentlig nøkkel brukes til å dekryptere.

Husk! Nøklene må alltid være fra samme nøkkelpar. I tilfelle 1 tilhører begge nøklene mottaker, mens i tilfelle to tilhører begge avsender.



Fra eksamen 2022: Asymmetrisk kryptering

For hver operasjon nedenfor angi riktig nøkkel:

1) Nøkkel sender benytter til signering (digital signatur)

2) Nøkkel mottager benytter for validerin (digital signatur)

3) Nøkkel sender benytter for kryptering (utveksling av hemmelig melding)

4) Nøkkel mottager benytter for dekryptering (utveksling av hemmelig melding)

Alternativer:

A. Senders private nøkkel
B. Mottagers private nøkkel
C. Senders offentlige nøkkel
D. Mottagers offentlige nøkkel

Fra eksamen 2022: Asymmetrisk kryptering

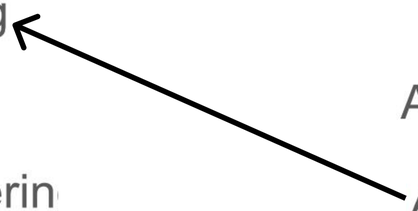
For hver operasjon nedenfor angi riktig nøkkel:

1) Nøkkel sender benytter til signering (digital signatur)

2) Nøkkel mottager benytter for validerin (digital signatur)

3) Nøkkel sender benytter for kryptering (utveksling av hemmelig melding)

4) Nøkkel mottager benytter for dekryptering (utveksling av hemmelig melding)



Alternativer:

A. Senders private nøkkel
B. Mottagers private nøkkel
C. Senders offentlige nøkkel
D. Mottagers offentlige nøkkel

Fra eksamen 2022: Asymmetrisk kryptering

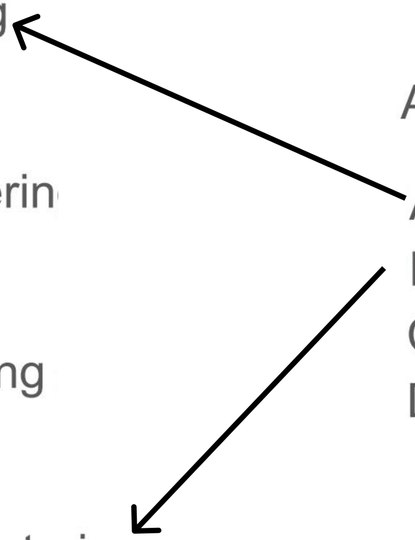
For hver operasjon nedenfor angi riktig nøkkel:

1) Nøkkel sender benytter til signering (digital signatur)

2) Nøkkel mottager benytter for validerin (digital signatur)

3) Nøkkel sender benytter for kryptering (utveksling av hemmelig melding)

4) Nøkkel mottager benytter for dekryptering (utveksling av hemmelig melding)



Alternativer:

A. Senders private nøkkel
B. Mottagers private nøkkel
C. Senders offentlige nøkkel
D. Mottagers offentlige nøkkel

Fra eksamen 2022: Asymmetrisk kryptering

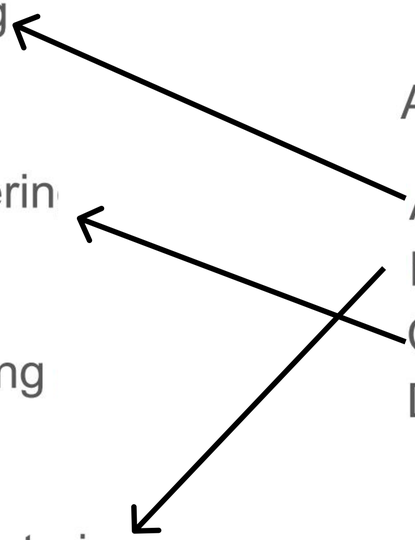
For hver operasjon nedenfor angi riktig nøkkel:

1) Nøkkel sender benytter til signering (digital signatur)

2) Nøkkel mottager benytter for validerin (digital signatur)

3) Nøkkel sender benytter for kryptering (utveksling av hemmelig melding)

4) Nøkkel mottager benytter for dekryptering (utveksling av hemmelig melding)



Alternativer:

A. Senders private nøkkel
B. Mottagers private nøkkel
C. Senders offentlige nøkkel
D. Mottagers offentlige nøkkel

Fra eksamen 2022: Asymmetrisk kryptering

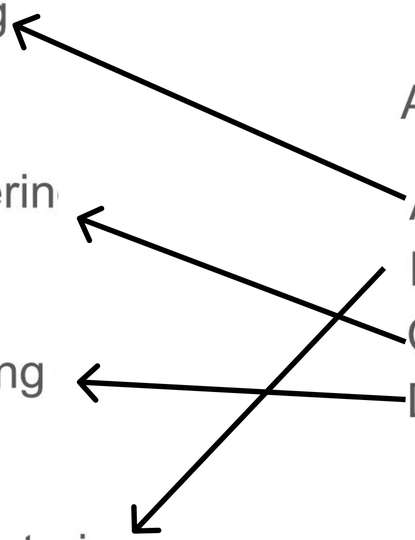
For hver operasjon nedenfor angi riktig nøkkel:

1) Nøkkel sender benytter til signering (digital signatur)

2) Nøkkel mottager benytter for validerin (digital signatur)

3) Nøkkel sender benytter for kryptering (utveksling av hemmelig melding)

4) Nøkkel mottager benytter for dekryptering (utveksling av hemmelig melding)

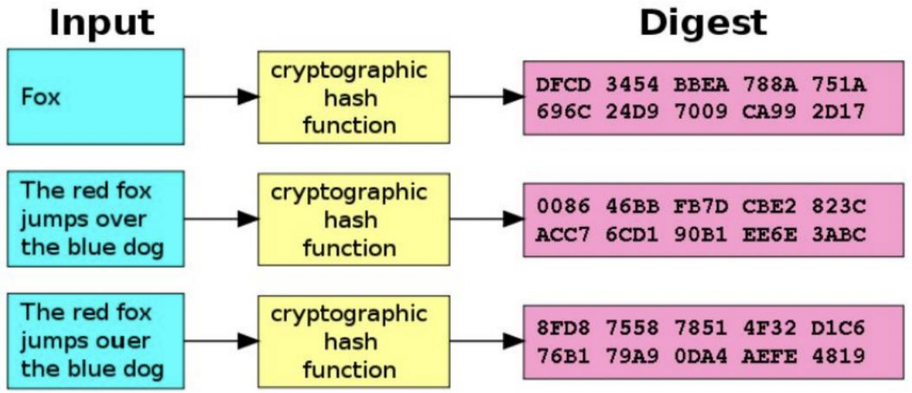


Alternativer:

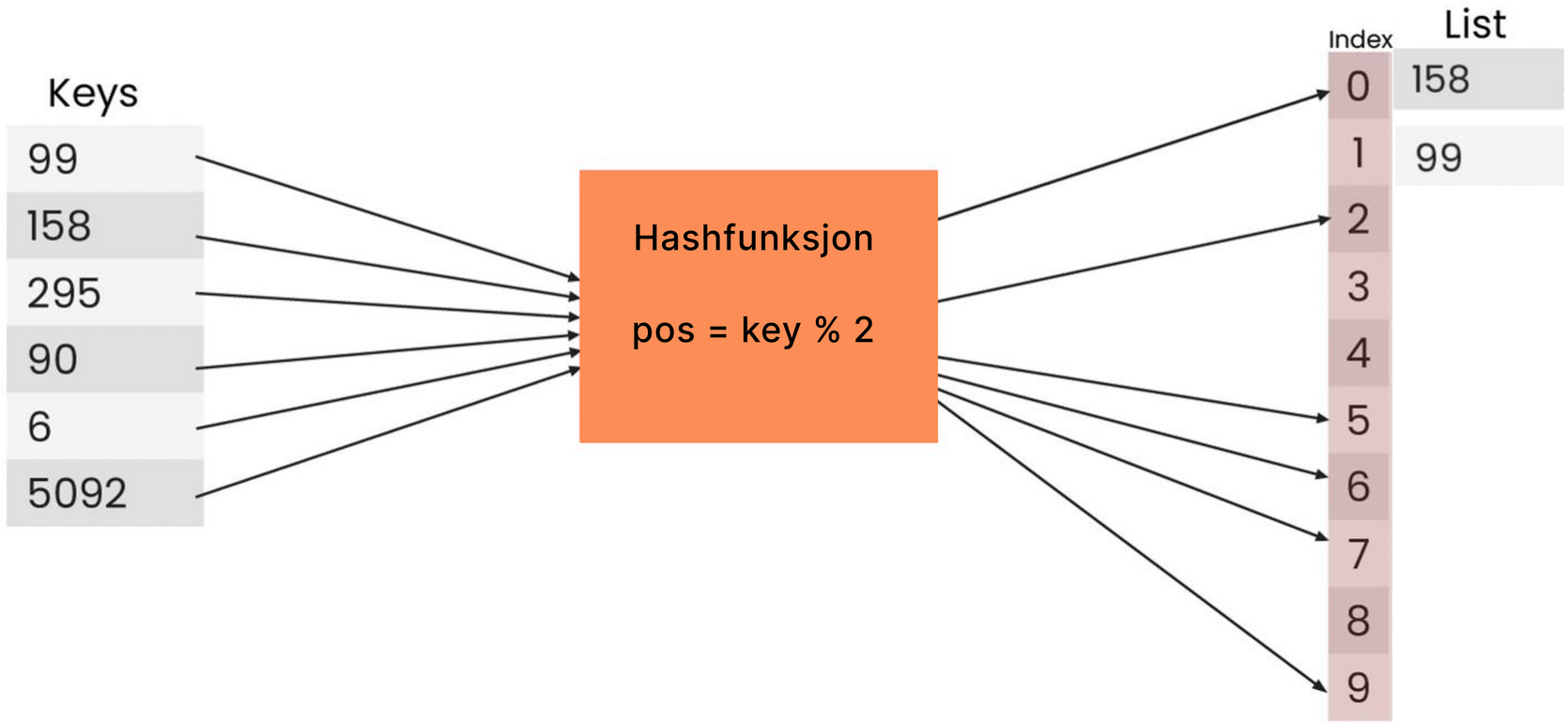
A. Senders private nøkkel
B. Mottagers private nøkkel
C. Senders offentlige nøkkel
D. Mottagers offentlige nøkkel

Hash-funksjoner

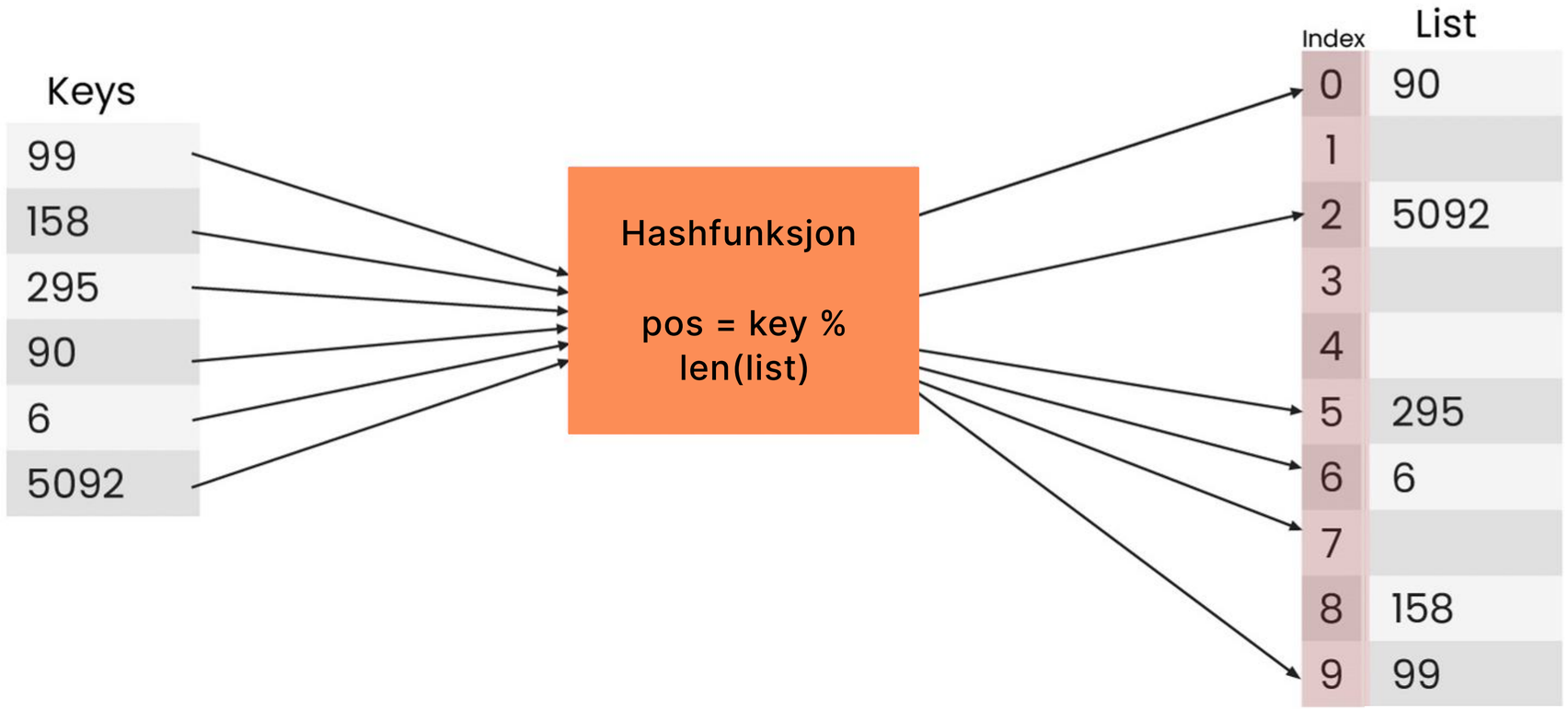
- I motsetning til de to andre typene kryptering er ikke hash-funksjoner laget for dekryptering.
- Funksjonen scrambler dataen på en måte som er umulig å reversere og du ender opp med en blokk med data, som blir lik hver gang du gir samme input.
- Outputen er like stor uansett om du mater funksjonen med ett ord, en setning eller en hel bok. Endrer du én bokstav i inputen blir outputen forskjellig.
- Hash brukes ofte for sjekksum-operasjoner og i passordtjenester, slik at databaser aldri lagrer passord i klartekst, men dette har også sårbarheter sikkerhetsmessig...



Finnes ulike måter å hashe på



Finnes ulike måter å hashe på



Ukeoppgave 11: hash-kryptering (sjekksumalgoritme)

Hash-kryptering er kryptering uten nøkler.

a) I forbindelse med hash-kryptering nevnes ofte «message-digest» eller «hash-digest». Hvorfor brukes dette som uttrykk?

b) Du jobber som utvikler og teamet ditt er i ferd med å bygge en nettside. Besøkende på nettsiden kan registrere seg med e-post og lage et passord for å opprette en brukerprofil på siden. Teamet ditt har forstått at det er en dårlig idé å lagre passordene til brukerne i klartekst, så dere vil i stedet benytte en hash-algoritme for å kryptere passordene. Er dette en god idé? Hvilke svakheter kan dere identifisere med denne strategien?

c) Hvilke sikkerhetsmål er hash-algoritmer med på å ivareta?

Ukeoppgave 11: hash-kryptering (sjekksumalgoritme) Fasit

Hash-kryptering er kryptering uten nøkler.

a) Hash algoritmer “fordøyer” data ned til en streng som har fast lengde (ofte 16, 32 eller 64 bit og i heksadesimal)

b) Dersom to brukere har samme passord, har de den samme hashen. Det finnes databaser med hashene til vanlige passord, så hvis brukerne deres benytter dårlige passord kan trusselaktører søke opp hashene deres i disse databasene og finne en match. Teamet ditt burde egentlig ikke prøve å lagre brukeres passord selv. Benytt heller google eller facebook (eller andre tilbydere av autentiseringstjenester) til å gjøre det for dere.

c) Først og fremst integritet, men også konfidensialitet ved at passord ikke lagres i klartekst og ikke kan leses av uvedkommende.

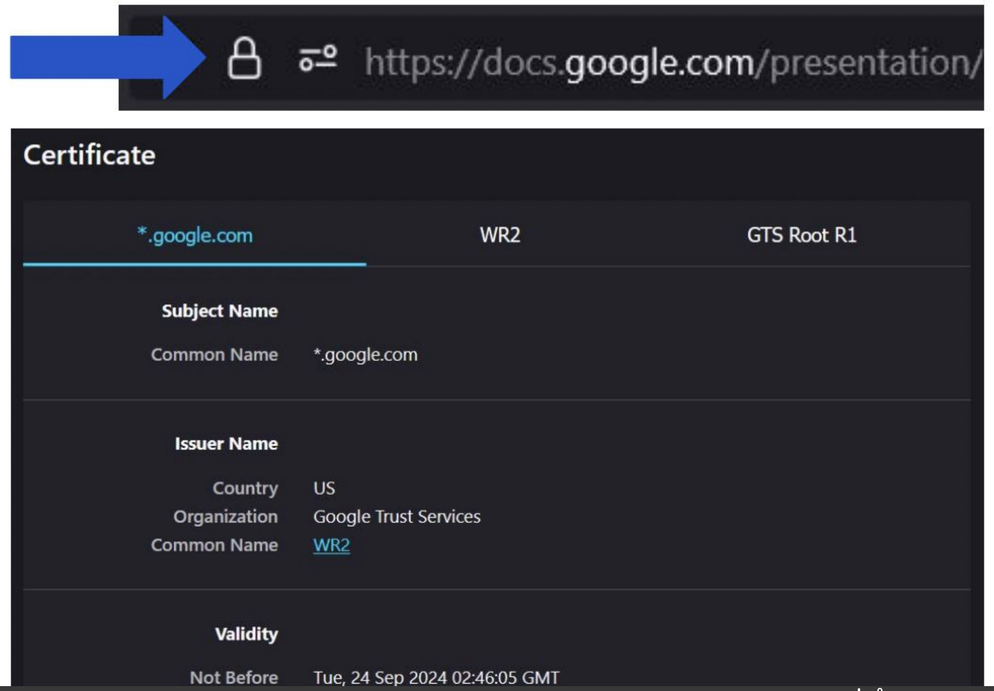
PKI (Public key infrastructure)

Offentlige nøkler er et potensielt svakt punkt i kryptering, derfor brukes PKI for å ha **rammeverk rundt distribuering av offentlige nøkler**, fra tiltrodde tjenere.

Offentlige nøkler kommer med et **sertifikat** som inneholder nøkkelen samt info, slik som f.eks. når nøkkelen går ut på dato og hvilken autoritet som utstedet sertifikatet.

Det **bygger på tillit til autoriteter**. Tjenesten er bedømt som autentisk av en autoritet. Denne autoriteten er bedømt autentisk av En enda høyere autoritet.

Husk! Et sertifikat betyr IKKE nødvendigvis at tjenesten ikke er ondsinnet. Kun at den er autentisk.



15 Minutter pause

Selvstendig arbeid

Spør om hjelp hvis dere lurer på noe :-)

Takk for i dag!

- aanundj@uio.no

Sees neste uke