Mentimeter

# !!! Takeover !!!

If "gruppelærere":
--> Hvem er vi?
--> "Street knowledge"
--> pEnSuM

Else:
--> exit()

5

Mentimeter

# Hvem er vi?

victou@ifi.uio.no
embrikht@ifi.uio.no

4

Mentimeter

# Street knowledge

2

Mentimeter



Mentimeter

# Før eksamen

- Løse mange oppgaver
- MINIMUM 1 eksamenssett
- Bli kjent med formatet
- Forbered GODE hjelpemidler
- Slapp av ;)

Mentimeter

# Format på oppgavene

- Sjekk om du skal huke av ett eller flere alternativer
- Sjekk om du trekk for galt svar, dette avgjør om du bør "gjette".

Mentimeter

HyperText Markup Language (HTML) er et markeringsspråk for formatering av nettsider der man blant mye annet kan vise tekst i forskjellige farger. I HTML representeres farger med en rød (R), grønn (G) og blå (B) verdi - såkalt RGB. Disse er vanligvis angitt i hexadesimal notasjon, der den første byten (fra venstre) er rød, den andre er grønn, og den tredje er blå.

Hvilke verdier for rød, grønn og blå har fargekoden 0xA07CD1?



**Velg ett eller flere alternativer**

- [ ] rød=148, grønn=124, blå=209
- [ ] rød=148, grønn=128, blå=191
- [ ] rød=160, grønn=134, blå=179
- [ ] rød=160, grønn=124, blå=209

Du har følgende to bytes:

Byte A:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |

Byte B:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |

Regn ut en ny byte C som er summen av disse (C = A + B). Hvilke verdier kan C ha?

**Velg ett eller flere alternativer**

- [ ] -99
- [ ] 157
- [ ] -67
- [ ] 126

Mentimeter

# 1.3 Tallsystemer

Konverter til desimal (10-tall) systemet.

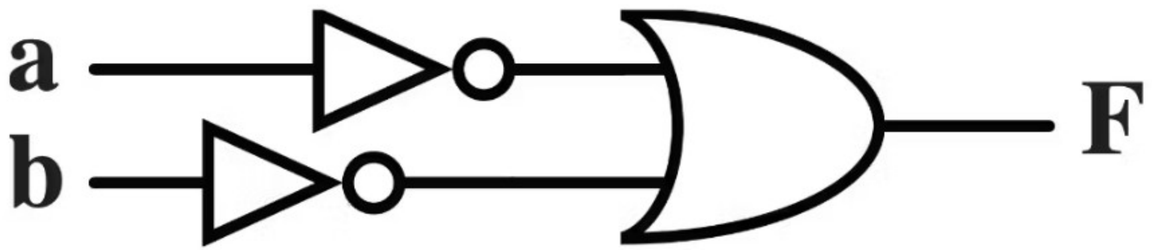
a) $1101_2$ Velg alternativ (Ingen av disse, 23, 51, 13, 135)

b) $113_4$ Velg alternativ (23, 13, Ingen av disse, 135, 51)

c) 0x33 Velg alternativ (51, 23, Ingen av disse, 13, 135)

d) $207_8$ Velg alternativ (51, 23, 135, Ingen av disse, 13)

Mentimeter




Funksjonsuttrykket for kretsen over er:

**Velg ett eller flere alternativer:**

- $F = \overline{a} + \overline{b}$
- $F = \overline{a} \cdot \overline{b}$
- $F = \overline{(ab)}$
- $F = \overline{a + b}$

Mentimeter

Konfidensialitet er et sentralt krav i norsk personvernlovgivning. Hvilke av følgende sikkerhetstiltak kan sørge for å ivareta konfidensialitet for persondata som behandles i et IT-system:

**Velg ett eller flere alternativer**

- [ ] Bruk av kryptografi for data lagret i systemet
- [ ] Sørge for redundante tjenester
- [ ] Bruk av skallforsvar
- [ ] Sørge for sikkerhetskopi av alle data
- [ ] Sørge for sikkerhetskopi av all maskinvare
- [ ] Identifisere alle brukere av IT-systemet

Mentimeter

# Gode hjelpemidler

Mentimeter

| Kode | Navn | Beskrivelse |
|---|---|---|
| 0xx | HLT | Stopper eksekveringen |
| 1xx | ADD | Adderer verdien i angitt minnelokasjon med akkumulatoren |
| 2xx | SUB | Subtraherer verdien i angitt minnelokasjon med akkumulatoren |
| 3xx | STA | Lagrer akkumulatoren i angitt minnelokasjon |
| 4xx | - | Ikke i bruk |
| 5xx | LDA | Henter verdi fra minnet til akkumulatoren |
| 6xx | BRA | Hopper til angitt adresse |
| 7xx | BRZ | Hopper hvis akkumulatoren er 0 |
| 8xx | BRP | Hopper hvis akkumulatoren er ≥ 0 |
| 901 | INP | Leser verdi fra input, og legger svaret i akkumulatoren |
| 902 | OUT | Skriver ut verdien i akkumulatoren |
| 922 | OTC | Skriver ut ASCII-tegn (ikke i boka) |

Mentimeter

# ASCII

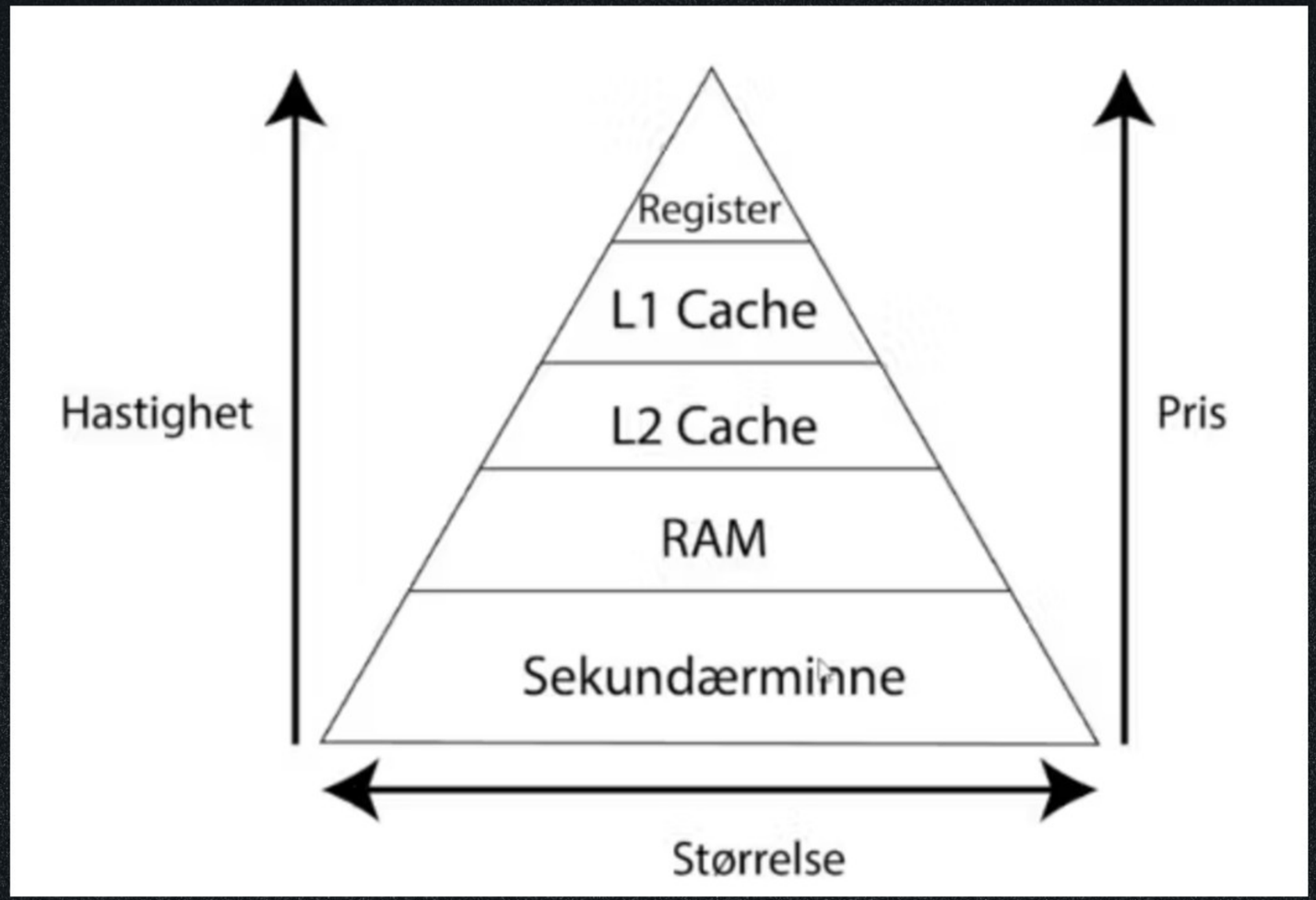
Første vellykkede forsøk på standardisering var ASCII (American Standard Code for Information Interchange) i 1963; den har 128 tegn:

**ASCII Code Chart**

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | NUL | SOH | STX | ETX | EOT | ENQ | ACK | BEL | BS | HT | LF | VT | FF | CR | SO | SI |
| 1 | DLE | DC1 | DC2 | DC3 | DC4 | NAK | SYN | ETB | CAN | EM | SUB | ESC | FS | GS | RS | US |
| 2 | | ! | " | # | $ | % | & | ' | ( | ) | * | + | , | - | . | / |
| 3 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | : | ; | < | = | > | ? |
| 4 | @ | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 5 | P | Q | R | S | T | U | V | W | X | Y | Z | [ | \ | ] | ^ | _ |
| 6 | ` | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o |
| 7 | p | q | r | s | t | u | v | w | x | y | z | { | \| | } | ~ | DEL |

1

Mentimeter

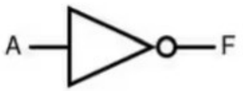

Register
L1 Cache
L2 Cache
RAM
Sekundærminne
Hastighet
Pris
Størrelse

Mentimeter

INV - port

$F = A'$

| A | F |
|---|---|
| 0 | 1 |
| 1 | 0 |




OR - port

$F = A+B$

| A | B | F |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |




AND - port

$F = AB$

| A | B | F |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |




NOR - port

$F = (A + B)'$

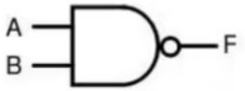
| A | B | F |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 0 |




NAND - port

$F = (AB)'$

| A | B | F |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |




XOR - port

$F = A \oplus B$

| A | B | F |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |




XNOR - port

$F = (A \oplus B)'$

| A | B | F |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |




## Alle logiske port-typer

1

Mentimeter

## Boolean algebra simplification rules

| | | |
|---|---|---|
| 1. | Law of Identity | $\overline{A} = \overline{A}$<br>$\overline{\overline{A}} = \overline{\overline{A}}$ |
| 2. | Commutative Law | $A \cdot B = B \cdot A$<br>$A + B = B + A$ |
| 3. | Associative Law | $A \cdot (B \cdot C) = A \cdot B \cdot C$<br>$A + (B + C) = A + B + C$ |
| 4. | Idempotent Law | $A \cdot A = A$<br>$A + A = A$ |
| 5. | Double Negative Law | $\overline{\overline{A}} = A$ |
| 6. | Complementary Law | $A \cdot \overline{A} = 0$<br>$A + \overline{A} = 1$ |
| 7. | Law of Intersection | $A \cdot 1 = A$<br>$A \cdot 0 = 0$ |
| 8. | Law of Union | $A + 1 = 1$<br>$A + 0 = A$ |
| 9. | DeMorgan's Theorem | $\overline{AB} = \overline{A} + \overline{B}$<br>$\overline{A + B} = \overline{A}\,\overline{B}$ |
| 10. | Distributive Law | $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$<br>$A + (BC) = (A + B) \cdot (A + C)$ |
| 11. | Law of Absorption | $A \cdot (A + B) = A$<br>$A + (AB) = A$ |
| 12. | Law of Common Identities | $A \cdot (\overline{A} + B) = AB$<br>$A + (\overline{A}B) = A + B$ |

Mentimeter

# Selve dagen

- Klær
- Transport
- Passord og brukernavn
- Ta med deg det du MÅ ha
- !!! MOBILEN / ALARM !!!
- 5 minutter før eksamen starter
- 30 min etter eksamensstart

2

Mentimeter

# På eksamen

- Se gjennom eksamen og notér oppgaver til trøsterunde
- Hvis du får tekniske problemer, kontakt IT-vaktene
- Luftetur er lov :)
- Svar noe på alle oppgaver!

Hva hvis man ikke skjønner oppgaven?
- Eliminere alternativer
- Ta utgangspunkt i ting du er sikker på

1

Mentimeter

# Digital Representasjon

1

Mentimeter

| Desimal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Hex | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |

1

Mentimeter

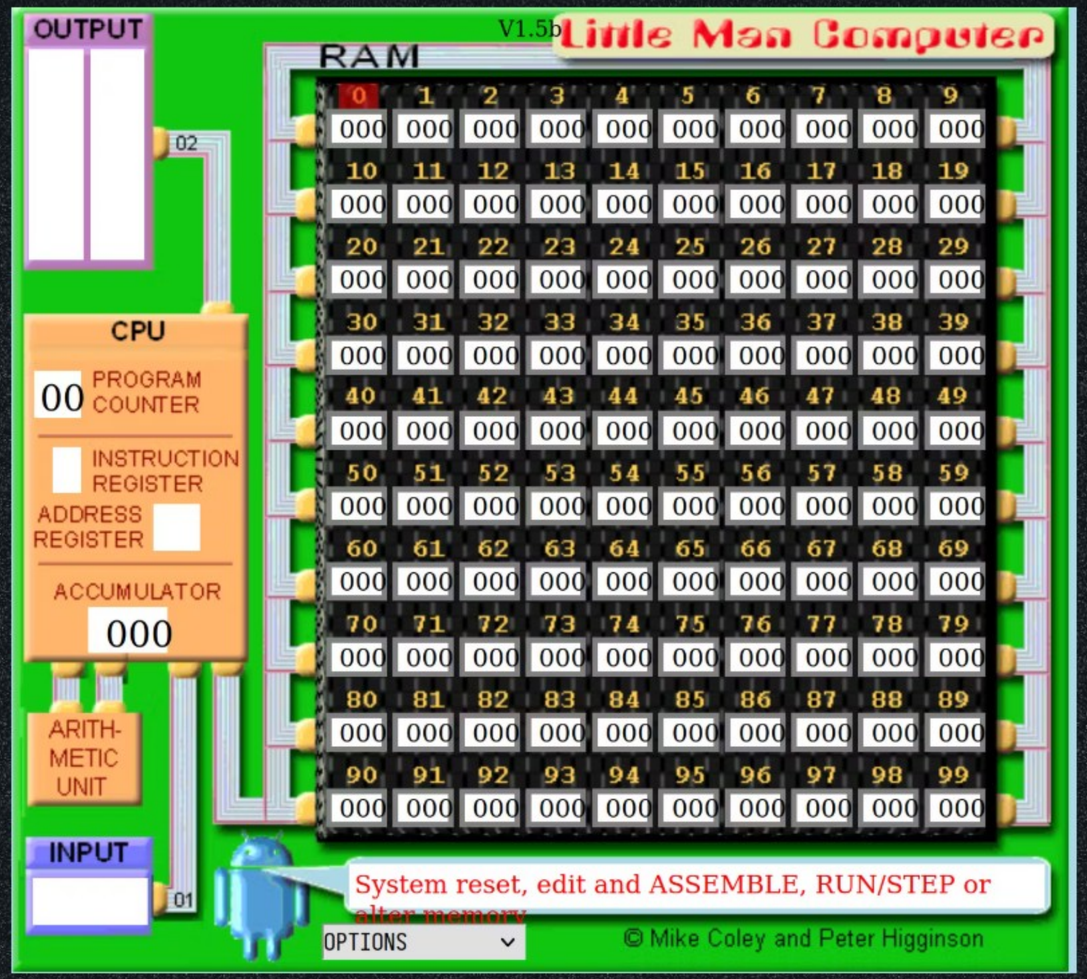
$10010111_2 = ?_{10}$

| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|
| $1 * 2^7$ | $0 * 2^6$ | $0 * 2^5$ | $1 * 2^4$ | $0 * 2^3$ | $1 * 2^2$ | $1 * 2^1$ | $1 * 2^0$ |
| 128 | 0 | 0 | 16 | 0 | 4 | 2 | 1 |

$128 + 16 + 4 + 2 + 1 = 151$

$10010111_2 = 151_{10}$

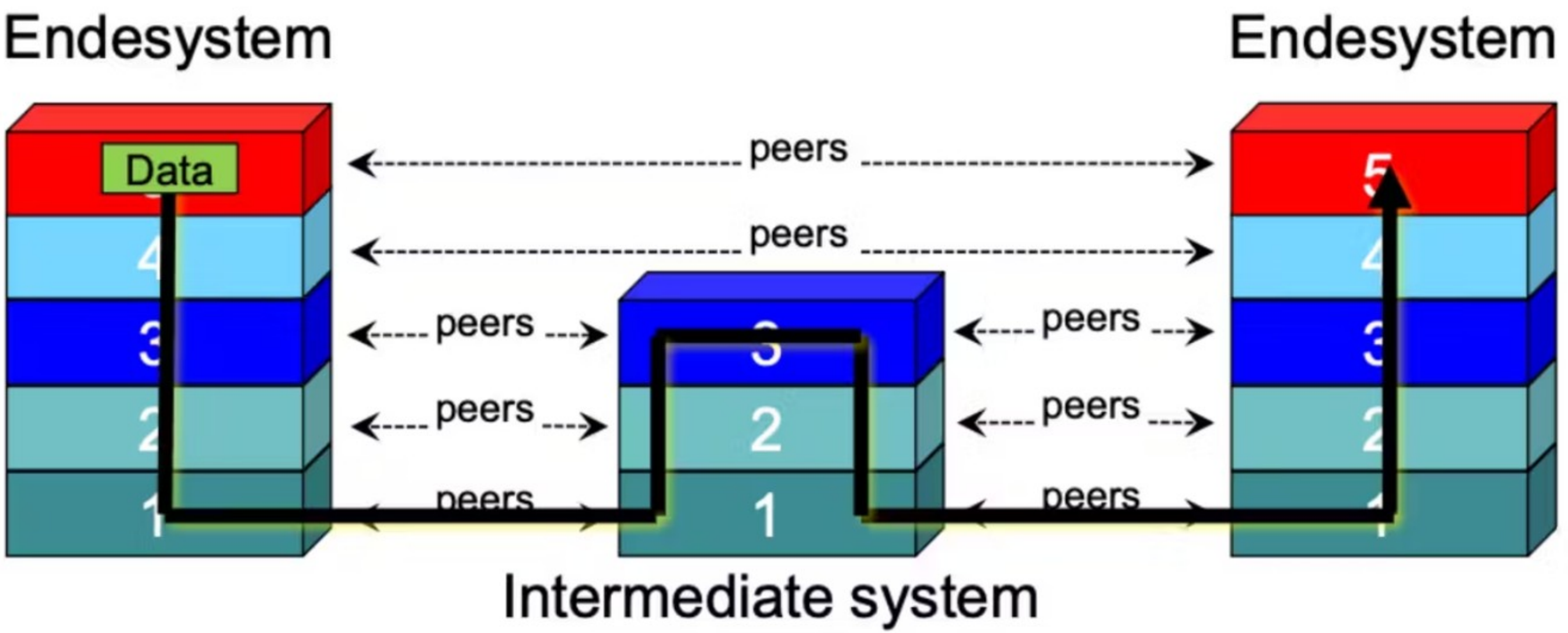
1


OUTPUT
V1.5b
Little Man Computer
RAM
0 1 2 3 4 5 6 7 8 9
000 000 000 000 000 000 000 000 000 000
10 11 12 13 14 15 16 17 18 19
000 000 000 000 000 000 000 000 000 000
20 21 22 23 24 25 26 27 28 29
000 000 000 000 000 000 000 000 000 000
30 31 32 33 34 35 36 37 38 39
000 000 000 000 000 000 000 000 000 000
40 41 42 43 44 45 46 47 48 49
000 000 000 000 000 000 000 000 000 000
50 51 52 53 54 55 56 57 58 59
000 000 000 000 000 000 000 000 000 000
60 61 62 63 64 65 66 67 68 69
000 000 000 000 000 000 000 000 000 000
70 71 72 73 74 75 76 77 78 79
000 000 000 000 000 000 000 000 000 000
80 81 82 83 84 85 86 87 88 89
000 000 000 000 000 000 000 000 000 000
90 91 92 93 94 95 96 97 98 99
000 000 000 000 000 000 000 000 000 000
02
CPU
00 PROGRAM COUNTER
INSTRUCTION REGISTER
ADDRESS REGISTER
ACCUMULATOR
000
ARITH-METIC UNIT
INPUT
01
System reset, edit and ASSEMBLE, RUN/STEP or alter memory
OPTIONS
© Mike Coley and Peter Higginson

Mentimeter

# Nettverk

Mentimeter


Endesystem
Endesystem
Data
peers
peers
peers
peers
peers
peers
peers
peers
5
4
3
2
1
3
2
1
Intermediate system

Mentimeter

- To måter å oppgi en IP-adresse på:
  - **Punktnotasjon**
    - F.eks. 192.168.1.0
      - Må da oppgi nettverksmasken
        - 255.255.255.0
  - **CIDR-notasjon**
    - Punktnotasjon + antall bits nettverksmasken består av
      - 192.168.1.0/24
    - Hvordan ser man antall bits nettverksmasken består av?
      - 255.255.255.0 = 11111111.11111111.11111111.00000000
        - Antall enere er 24

Mentimeter

# Sikkerhet

1

Mentimeter

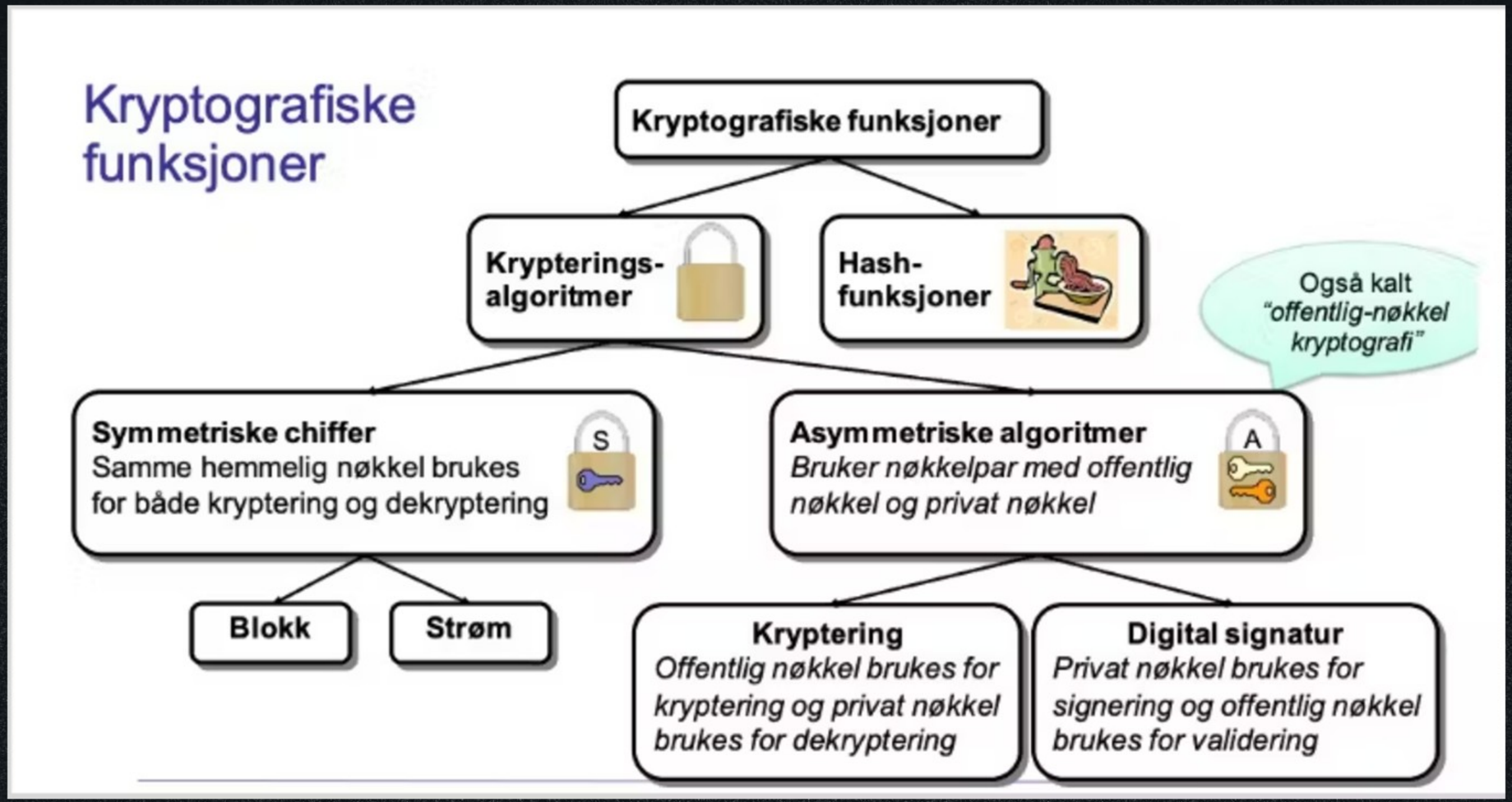
# Sikkerhetsmål

Sikkerhetsmål er egenskaper ved informasjonssikkerhet som vi ønsker å oppnå eller tilby. De opprinnelige sikkerhetsmålene er konfidensialitet, integritet og tilgjengelighet (KIT-målene)

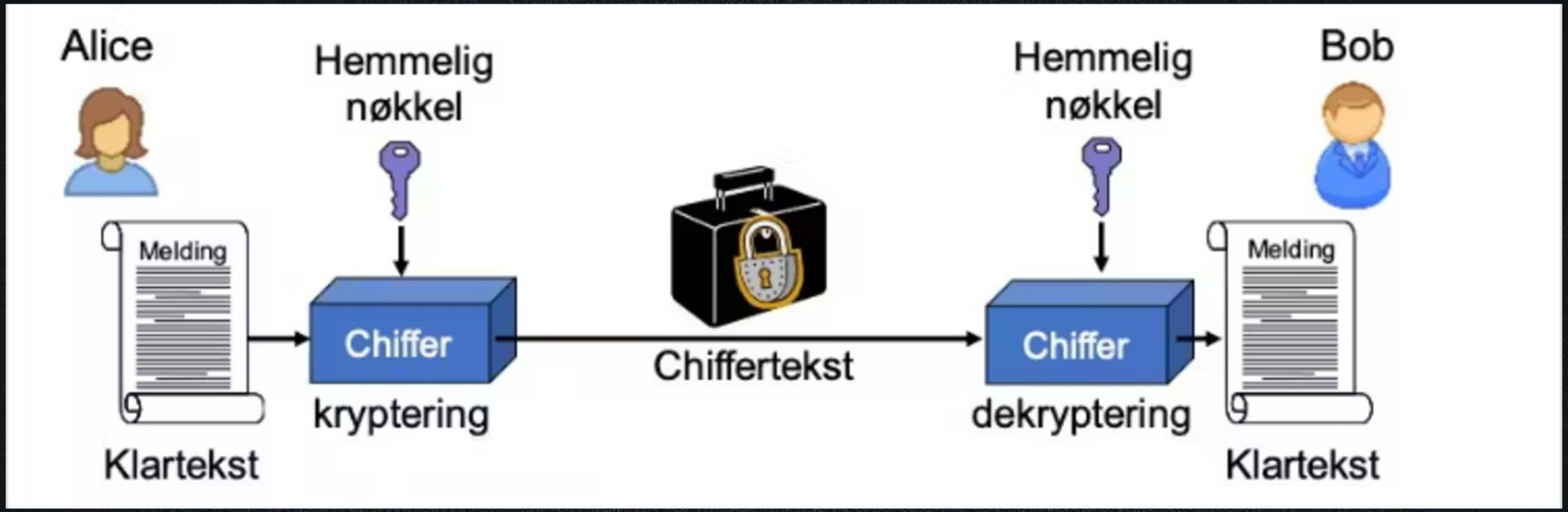
- **Konfidensialitet**
  - Å sikre at ingen andre enn de med rettmessig behov har tilgang til informasjon
- **Integritet**
  - Å sikre at informasjon alltid er korrekt og ikke endres eller slettes utilsiktet
- **Tilgjengelighet**
  - Å sikre at en informasjon alltid er tilgjengelig for rett person til rett tid

Mentimeter

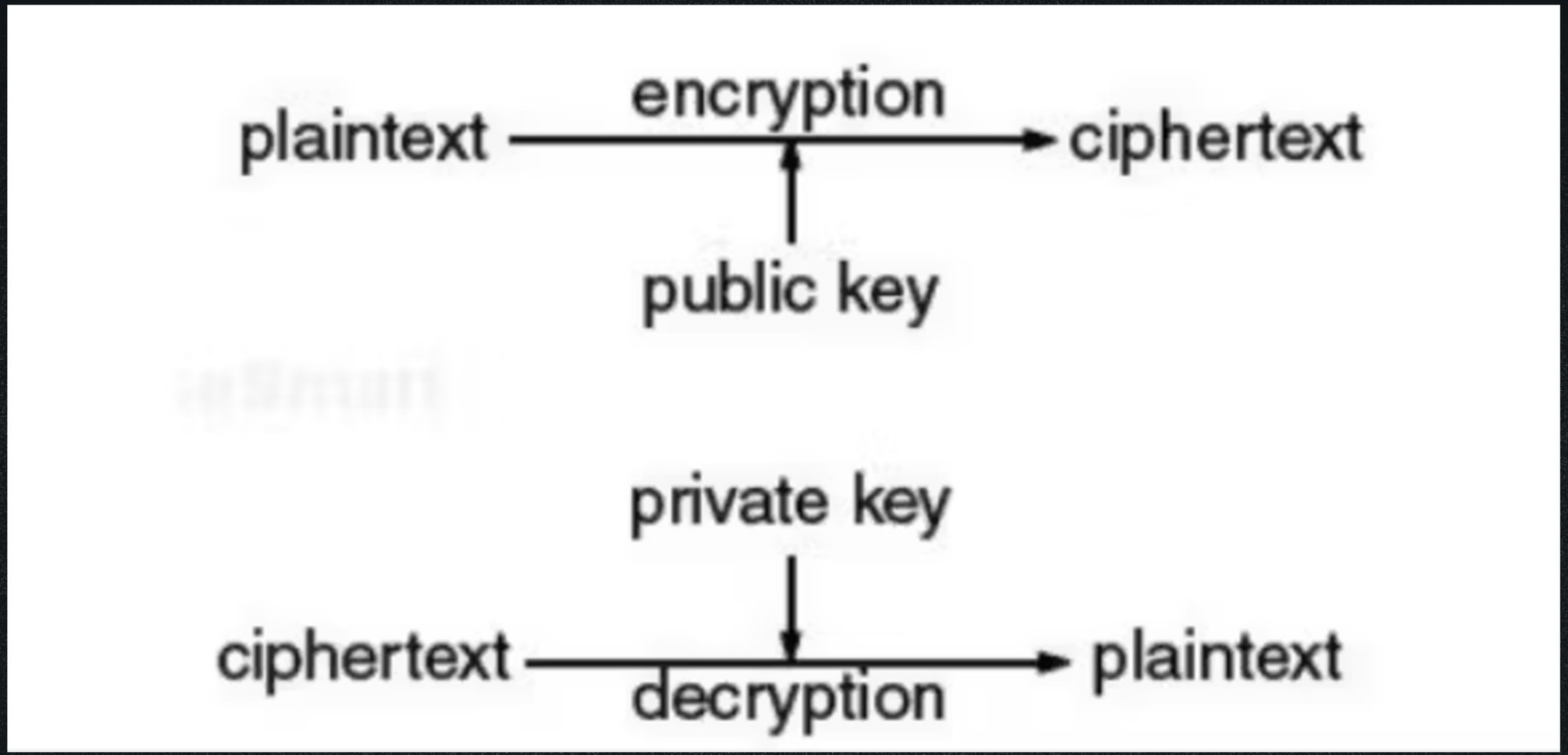
# Kryptografiske funksjoner



Mentimeter


Alice
Hemmelig nøkkel
Hemmelig nøkkel
Bob
Melding
Chiffer
Chiffertekst
Chiffer
Melding
kryptering
dekryptering
Klartekst
Klartekst

Mentimeter


plaintext
encryption
ciphertext
public key
private key
ciphertext
decryption
plaintext

Mentimeter

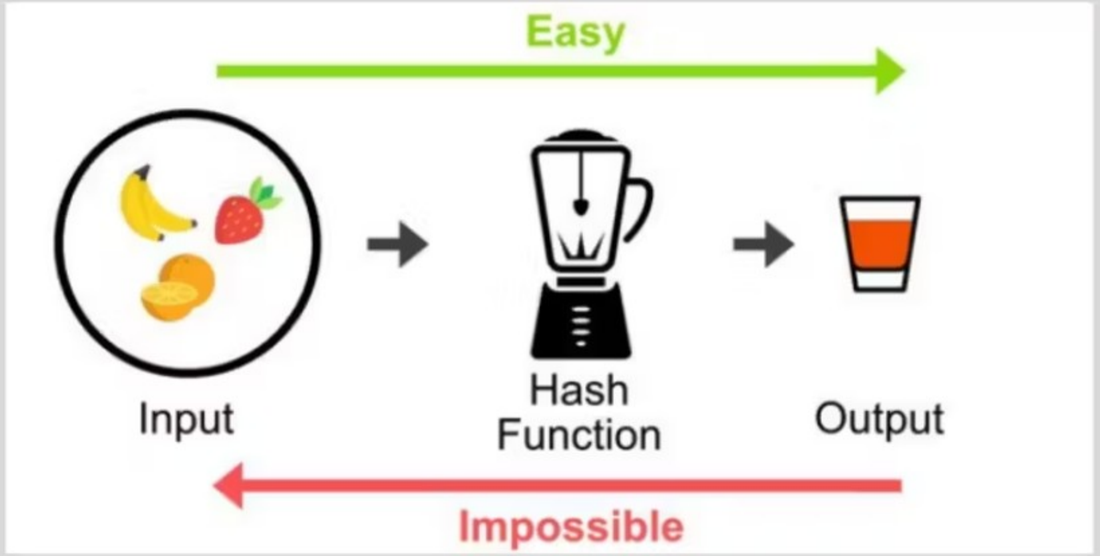
- Kriterier for en god sjekksumalgoritme/hashalgoritme:
  - Enkelt å regne ut sjekksum for en gitt beskjed
  - Ikke mulig å finne en beskjed for en gitt sjekksum
  - Ikke mulig å endre en beskjed uten at sjekksummen blir endret
  - Ikke mulig å finne to forskjellige beskjeder med samme sjekksum



Hashing



Hashing med salting

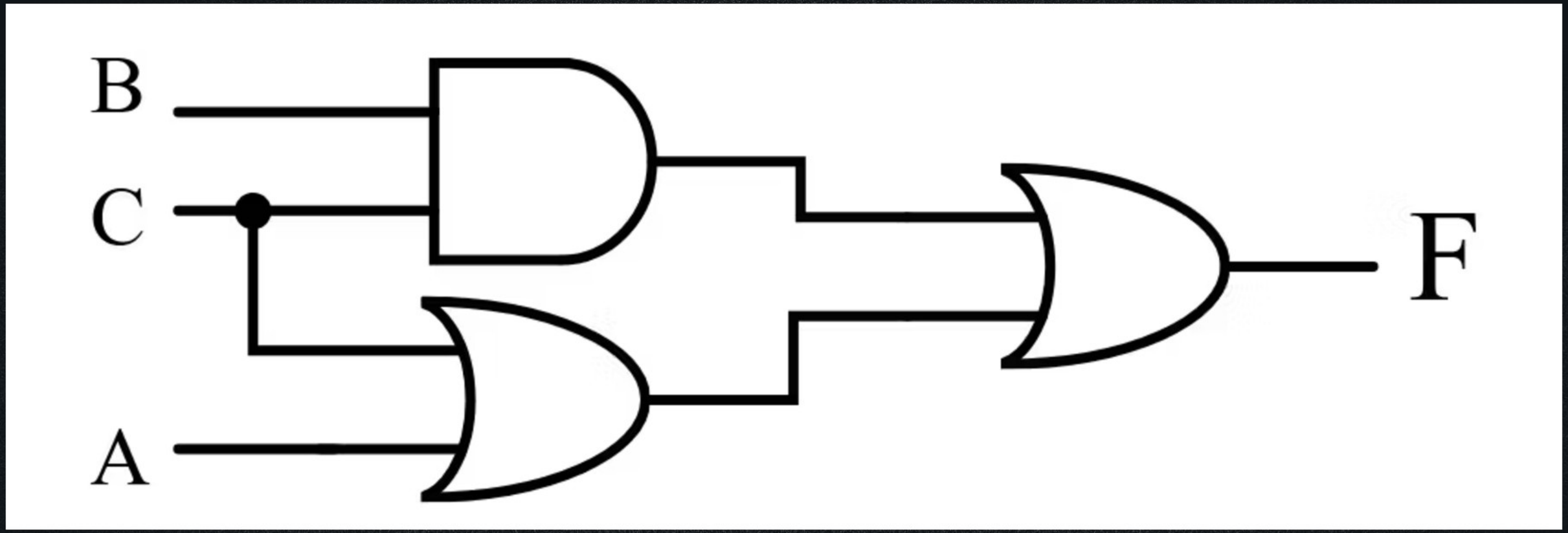



1

Mentimeter

# Maskinvare

Mentimeter



Mentimeter

**Er utsagnene sann eller usann?**

| | Sann | Usann |
|---|---|---|
| En transistor er en samling av strøm som utgjør 1 byte | ○ | ○ |
| Sekundærminne er flyktig minne | ○ | ○ |
| ALU ligger rett på utsiden av CPU | ○ | ○ |
| Når du får cache-miss betyr det at en del av minne er blitt ødelagt | ○ | ○ |
| Et register består av mange RAM | ○ | ○ |
| En databuss (BUS) frakter med seg informasjon mellom prosessoren og andre enheter | ○ | ○ |
| Den teknologiske utviklingen bidrar til færre transistorer på en chip | ○ | ○ |
| En full-adder kan brukes som subtraktor ved å ha mente-inn = 1 | ○ | ○ |
| Klokkesignalet i en CPU er lagret i RAM | ○ | ○ |
| En 64-bits ALU krever 65 stk av 1-bits ALU | ○ | ○ |

1

Mentimeter

7 **Kopi av Cache**

Anta at det er igjen 1000 instruksjoner og at en instruksjon tar 1 klokkesykel, bortsett fra eventuelle cache-miss. Videre kan du anta at det vil være 50% cache-miss hvor det vil ta totalt 10 klokkesykel for hver instruksjon i cache-miss.

Hvor lang til vil det totalt ta?

**Velg ett eller flere alternativer**

- [ ] 8250
- [ ] 5000
- [ ] 3000
- [ ] 7500
- [ ] 5500
- [ ] 13250
- [ ] 15000
- [ ] 6600
- [ ] 9000
- [ ] 10000

Mentimeter

# Spørsmål??

**13 questions**
**2 upvotes**

1

Mentimeter

# Takk for dette semesteret

På vegne av gruppelærere og rettere ønsker vi dere masse lykke til på eksamen! :)

1