



NTNU | Kunnskap for en bedre verden

# Morgendagens kryptografi

Jonathan Komada Eriksen - IIK, NTNU

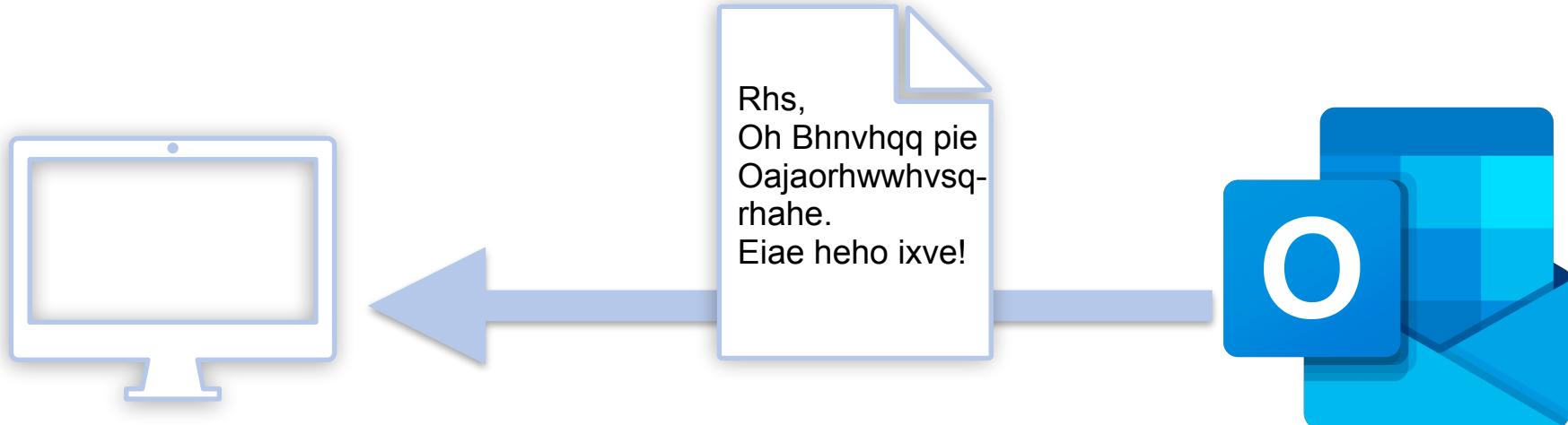
# Hva brukes kryptografi til?

## Holde informasjon sikker



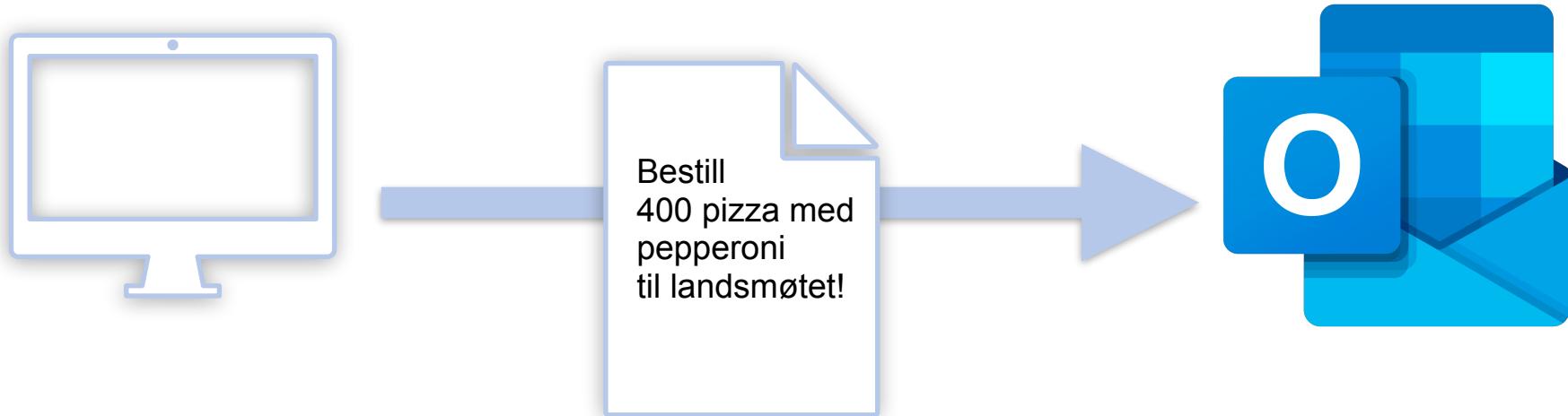
# Hva brukes kryptografi til?

## Holde informasjon sikker



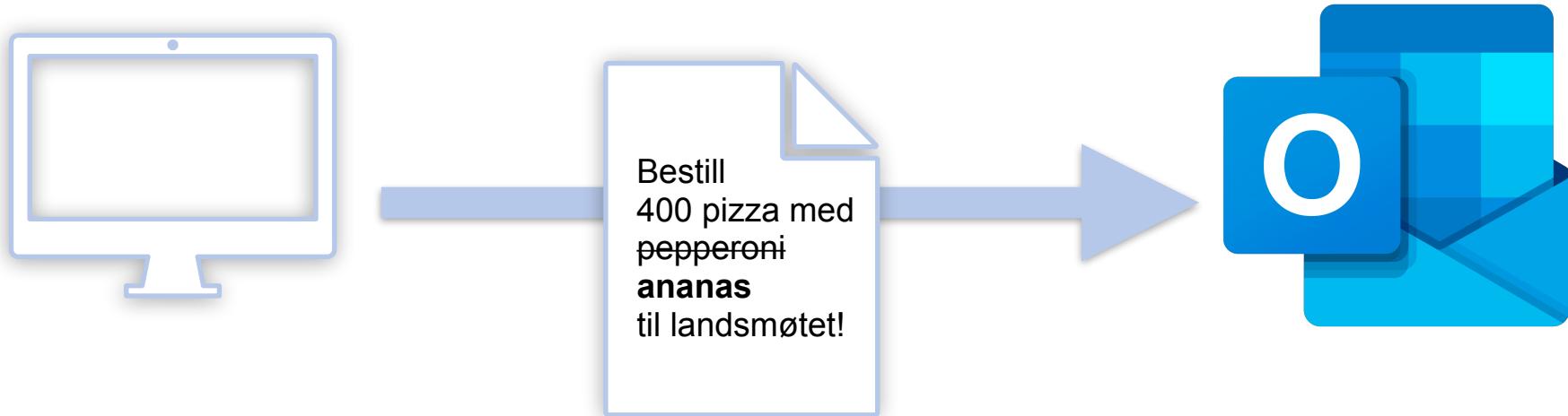
# Hva brukes kryptografi til?

## Holde informasjon sikker



# Hva brukes kryptografi til?

## Holde informasjon sikker



# Hva brukes kryptografi til?

Holde informasjon sikker ✓

- ALL DIGITALISERING er avhengig av at vi kan stole på kryptografi



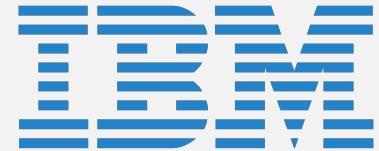
# Kvantemaskinens fremmarsj

QUANTUM COMPUTING

## New Algorithm Closes Quantum Supremacy Window

HARDWARE > QUANTUM | April 25, 2023 | updated 17 May 2023 8:36am

Investment in quantum technology hit a record \$2.35bn last year

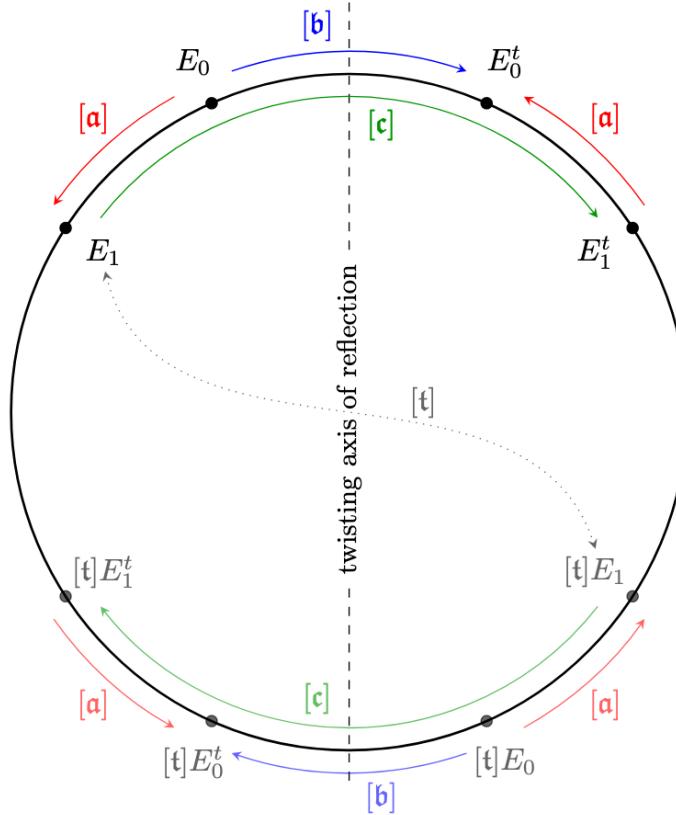


Real quantum computers.  
Right at your fingertips.

- En fundamentalt ny type datamaskin er her.
- En fullskala kvantemaskin knekker dagens kryptografi
  - **Ingen kryptografi → Ingen digital sikkerhet**

# Kvantesikker kryptografi

- Kryptografi må bygges opp fra bunn av.
- Mye arbeid gjenstår



# Dagens kryptografi er på overtid

- Kvantemaskiner store nok til å knekke dagens kryptografi (finnes? / er 5 år unna? / er 20 år unna?)
- Dine meldinger lagres nå, og dekrypteres i fremtiden.
  - **Tåler all e-post du får idag å havne hvor som helst om 5 år?**



**Enhver digitaliseringssstrategi må tenke på sikkerhet**  
...og den digitale sikkerheten må ta trusselen fra  
kvantemaskiner på alvor