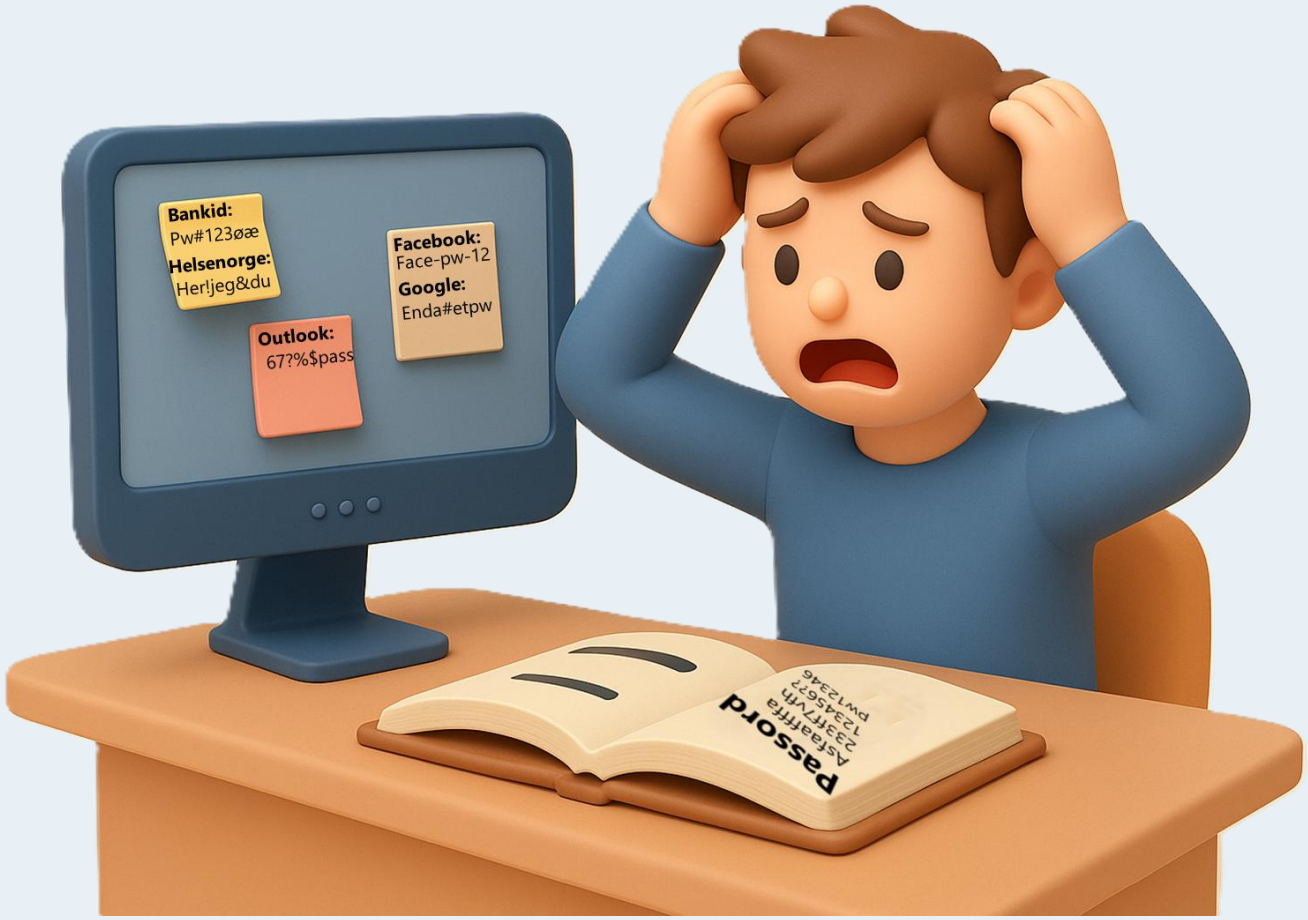
Seniornett
LARVIK



Passordene er på vei ut!

Velkommen til Passkey!

Sikker pålogging med passnøkkel og moderne biometrisk autentisering!

6. november 2025

By - AI&me - Stein Kristiansen Seniornett Larvik

Hva er Passkey?

Passkey består av et *kryptografisk* **nøkkelpar**:

- En **privat nøkkel** (hemmelig) som beviser hvem du.
  Denne lagres lokalt (sikkert) på enheten din, og du får tilgang til den med **biometri** eller **PIN**
- En **offentlig nøkkel**, som er **matematisk knyttet** til den *private nøkkelen*.
  Denne lagres på nettstedet/serveren.

Opprett en PASSKEY

- Du ønsker tilgang til et nettsted. Nettstedet støtter **passkey**-autentisering og sender en **forespørsel** til din enhet:

- Enheten din (f.eks. iPhone, Android, PC med Windows Hello) lager et nøkkelpar:
  - en **privat nøkkel** (lagres sikkert på enheten din), og
  - en **offentlig nøkkel**, som er matematisk knyttet til den private nøkkelen
  - Den offentlige nøkkelen sendes til nettstedet og lagres der sammen med *brukerIDen* din.

"Hei, jeg vil gjerne at du lager en passkey for brukeren din hos meg."

Hvor lagres nøkkelene?

Den private nøkkelen:

- På mobilen: I Secure Enclave (Apple) eller Trusted Execution Environment (Android).
- På PC: I TPM (Trusted Platform Module) eller Windows Hello-beskyttet lagring.
- På sikkerhetsnøkkel: I en fysisk FIDO2-kompatibel enhet (f.eks. YubiKey).

Ikke i skyen: Den *private* nøkkelen synkroniseres **aldri** til servere – skyen, men den kan synkroniseres mellom dine private enheter.

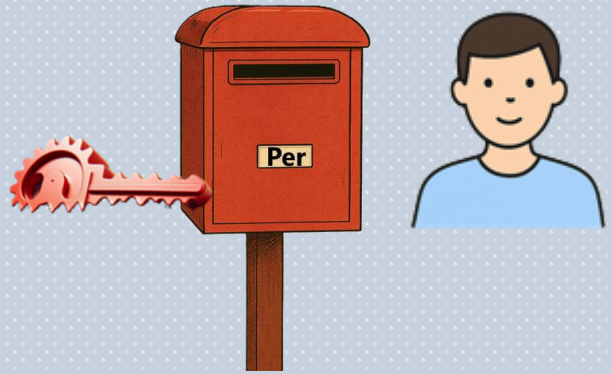
Den offentlige nøkkelen:

- På serveren – i skyen

Kryptografi

- Kryptering betyr å **gjøre en *melding*** eller et ***innhold*** **uleselig for andre**.
- Bare den som har riktig **nøkkel** kan låse den opp igjen.

“Som å legge et brev i en låst postkasse – alle kan putte inn, men bare eieren kan åpne.”



Litt (kryptografisk) historie

📜 Cæsar-kryptering (ca. 100 f.Kr.)

- **Hva:** En enkel metode der bokstaver forskyves i alfabetet (f.eks. A → D, B → E).
- Brukt av: Julius Cæsar for militære meldinger.
  Svakhet: Lett å knekke med frekvensanalyse eller prøv-og-feil.

🔑 Symmetrisk kryptering (1900-tallet)

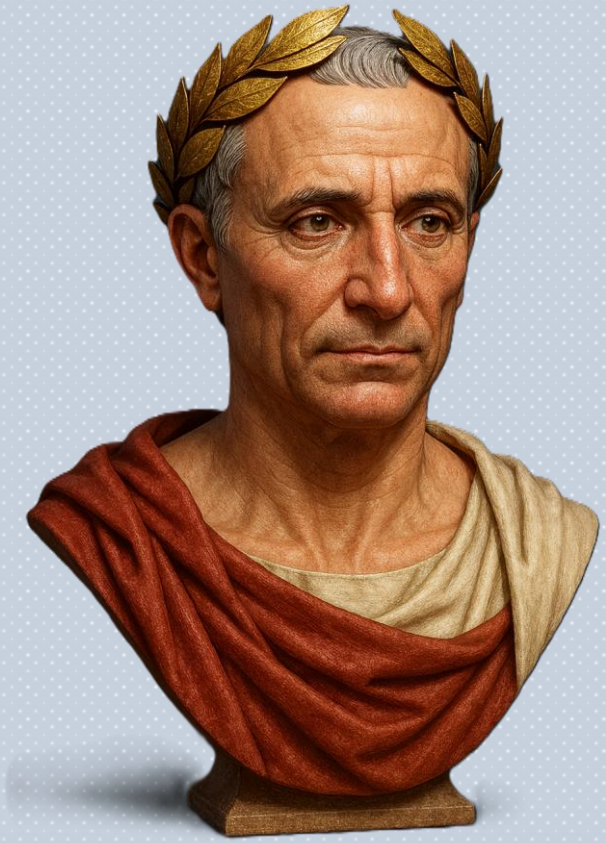
- **Hva:** Samme nøkkel brukes til både kryptering og dekryptering.
- Eksempel: DES (Data Encryption Standard) – utviklet på 1970-tallet.
  Svakhet: Nøkkelen må deles sikkert – vanskelig over internett.

🔐 AES (2001) – Moderne symmetrisk kryptering

- **Hva:** Avløseren til DES – rask, sikker og standard i dag.
- Brukt til: Kryptere filer, e-post, VPN, passordhvelv.
  Styrke: 128–256 bit nøkkel, svært vanskelig å knekke.

🔐🔓 RSA (1977) – Asymmetrisk kryptering

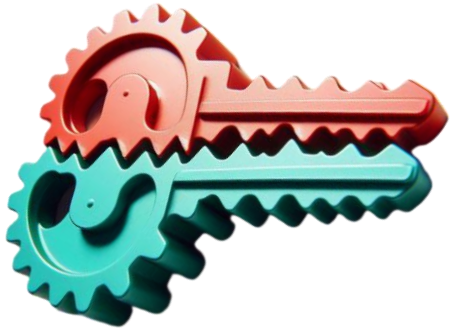
- **Hva**: Bruker to nøkler – én offentlig og én privat.
- **Brukt til**: Sikker nøkkelutveksling, digital signering.
  Styrke: Basert på matematiske problemer (primtallfaktorisering), meget vanskelig å knekke.



Kryptering vs. signering

🔒 Kryptering:

- Avsender bruker mottakerens **offentlige nøkkel**.
- Bare mottakeren (med **privat nøkkel**) kan åpne meldingen.
- Sikrer **konfidensialitet**.



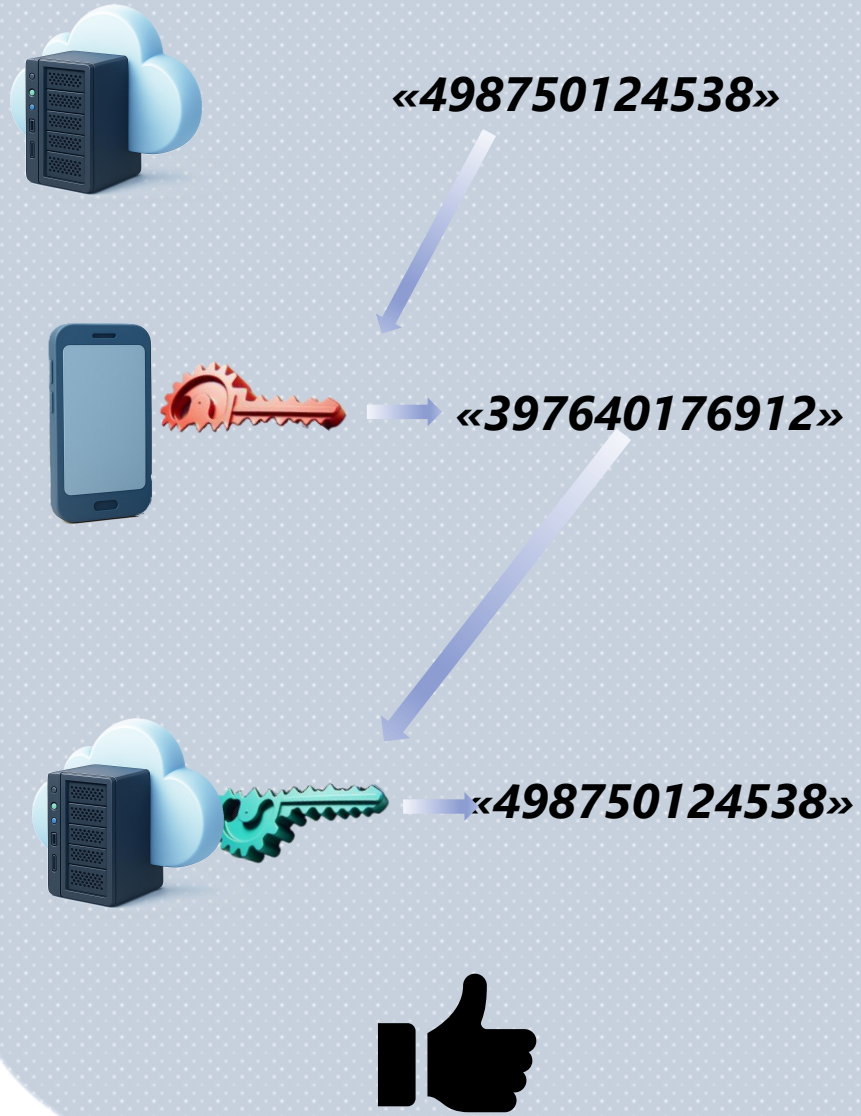
✍️ Signering:

- Avsender bruker sin **private nøkkel** til å signere data.
- Alle med den **offentlige nøkkelen** kan verifisere signaturen.
- Sikrer **autentisitet** og **integritet**.

Hvordan hentes nøkkelen ved verifisering?

1. **Nettstedet sender en challenge** – en tilfeldig kode som må signeres.
2. **Enheten spør deg om godkjenning** – via fingeravtrykk, ansikt eller PIN.
3. **Når du godkjenner**, får systemet tilgang til den private nøkkelen i den sikre modulen.
4. **Nøkkelen signerer challenge lokalt** – og sender signaturen tilbake til nettstedet.
5. **Nettstedet verifiserer signaturen** med den offentlige nøkkelen.

Du ser aldri nøkkelen selv – alt skjer automatisk og sikkert i bakgrunnen.



Asymmetrisk nøkkelpar – «enkelt» forklart

Velg to "store" primtall (i praksis i dag brukes tall som gir produkt på 617 desimal tall)
p = 32416190071
q = 32416187567

Beregn produktet
n = p × q = 1050809378732562746057

Beregn φ(n) (Eulers totient)
φ(n) = (p−1)(q−1) **=** 1050809378667720564420

Velg offentlig eksponent
e = 65537

Beregn privat eksponent
d = 48705916093281528347 3

Ferdige nøkler
Offentlig nøkkel: (e, n) **=** (65537, 1050809378732562746057)
Privat nøkkel: (d, n) **=** (48705916093281528347 3, 1050809378732562746057)

💡 Hele sikkerheten bygger på at det er **lett å gange p og q**,
men **ekstremt vanskelig å finne p og q igjen ut fra n**.

```
RSA-2048 = p x q =
25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357
```

Klar for en utfordring? Finn p og q begge primtall
Ingen har klart å faktorisere dette tallet per i dag.
Det var utlovet en dusør på $ 200.000 for den eller de som klarte dette først, men ingen klarte det.

Hva skjer når du mister tilgang til enheten?

- ✓ **Du kan *ikke* bruke passnøklene direkte**.
  Passnøkler er lagret på enheten og beskyttet med biometrisk autentisering (Face ID, Touch ID) eller enhetens passord.
- ✓ **Ingen synkronisering uten tilgang**.
  Hvis passnøklene ikke er synkronisert med en skytjeneste (som iCloud Keychain), er de kun tilgjengelige på den opprinnelige enheten.
- ✓ **Du kan bli låst ute fra kontoer**.
  Hvis du har konfigurert en konto til å bruke passnøkkel som eneste innloggingsmetode, og du ikke har tilgang til enheten, kan du ikke logge inn uten en alternativ metode.

Hva kan du gjøre?

- ✓ **Bruk en annen enhet med synkroniserte passnøkler.**
  Hvis du har aktivert synkronisering via iCloud Keychain, kan du bruke en annen Apple-enhet som er koblet til samme Apple-ID. Ingen synkronisering uten tilgang.
  Hvis passnøklene ikke er synkronisert med en skytjeneste (som iCloud Keychain), er de kun tilgjengelige på den opprinnelige enheten.
- ✓ **Gjenopprett enheten eller få tilgang via backup.**
  Hvis du har en sikkerhetskopi av enheten, kan du gjenopprette den på en ny enhet og få tilgang til passnøklene..
  Hvis du har konfigurert en konto til å bruke passnøkkel som eneste innloggingsmetode, og du ikke har tilgang til enheten, kan du ikke logge inn uten en alternativ metode.
- ✓ **Bruk alternative innloggingsmetoder.**
  Mange tjenester tilbyr backup-metoder som SMS, e-post eller engangskoder. Se etter “Logg inn på annen måte” eller “Har du problemer?” på innloggingssiden.
- ✓ **Kontakt kundestøtte.**
  Hvis du er låst ute fra en viktig konto, kan du kontakte tjenestens kundestøtte for hjelp med gjenoppretting.