NTNU | Kunnskap for en bedre verden

Kryptografi - Fortid, Nåtid og en Kvantesikker Fremtid

Jonathan Komada Eriksen - IIK, NTNU

Det enkle er ofte det beste?

KRYPTOGRAFI - FORTID

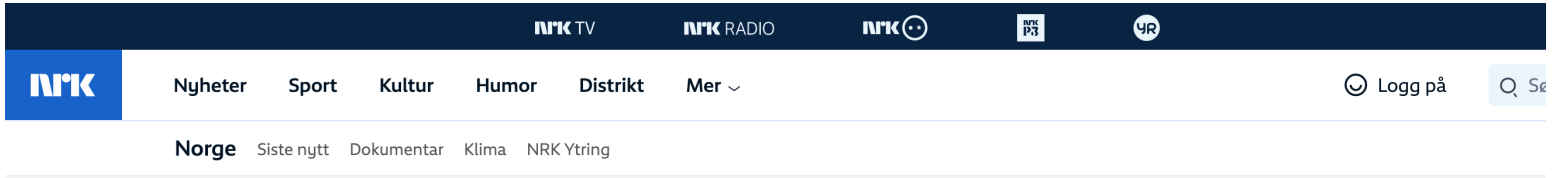
Historisk: Bok-Chiffer

Melding: Angrip imorgen

Historisk: Bok-Chiffer

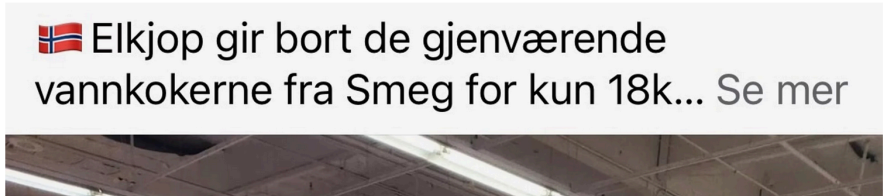
Melding: Angrip imorgen

Hemmelig nøkkel:



Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» reklamerte med råbillige vannkokere på Facebook.
Bak annonsen sto utenlandske kriminelle.



Snorre Tønset
Journalist

Historisk: Bok-Chiffer

Melding: Angrip imorgen **Chiffertekst: 2/8**

Historisk: Bok-Chiffer

Melding: Angrip imorgen **Chiffertekst: 2/8, 1/1**

Historisk: Bok-Chiffer

Melding: Angrip imorgen

Chiffertekst: 2/8, 1/1, 1/22

Historisk: Bok-Chiffer

Melding: Angrip imorgen

Chiffertekst: 2/8, 1/1, 1/22, 3/7

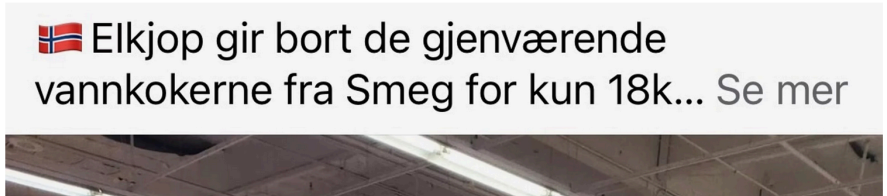
Historisk: Bok-Chiffer

Melding: Angrip imorgen

Chiffertekst: 2/8, 1/1, 1/22, 3/7, ...

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» reklamerte med råbillige vannkokere på Facebook.
Bak annonsen sto utenlandske kriminelle.



Snorre Tønset
Journalist

Historisk: Bok-Chiffer

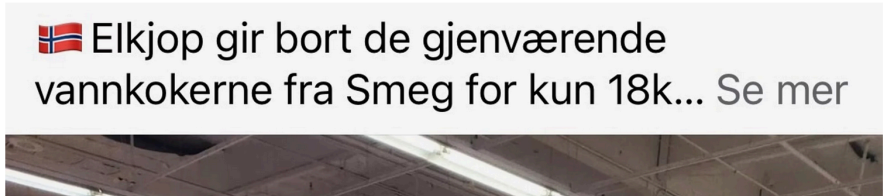
Melding: Angrip imorgen

Chiffertekst: 2/8, 1/1, 1/22, 3/7, ...

Fryktelig Kronglete

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» reklamerte med råbillige vannkokere på Facebook.
Bak annonsen sto utenlandske kriminelle.

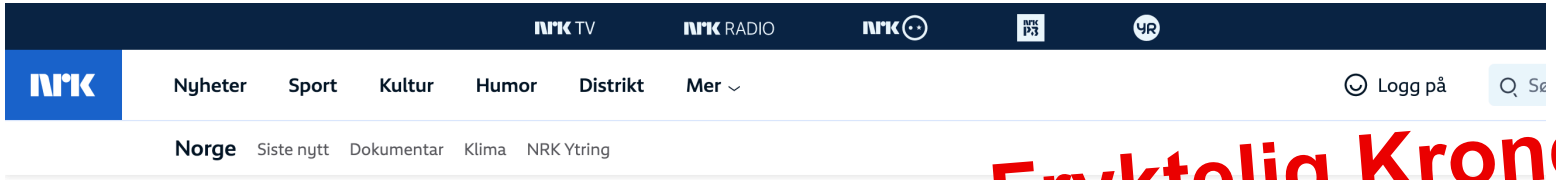


Snorre Tønset
Journalist

Historisk: Bok-Chiffer

Melding: Angrip imorgen

Chiffertekst: 2/8, 1/1, 1/22, 3/7, ...

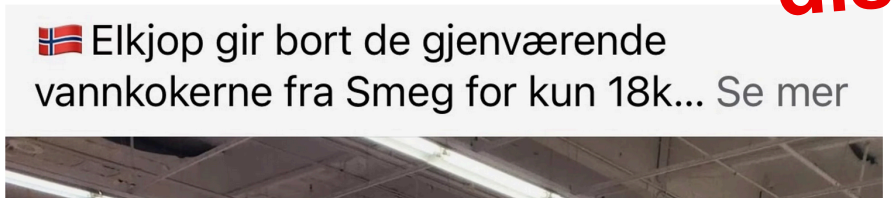


Fryktelig Kronglete

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

Store, vanskelig å distribuere, nøkler

«Elkjøp» reklamerte med råbillige vannkokere på Facebook. Bak annonsen sto utenlandske kriminelle.



Snorre Tønset
Journalist

Symmetrisk Kryptografi

~1940

Symmetrisk Kryptografi

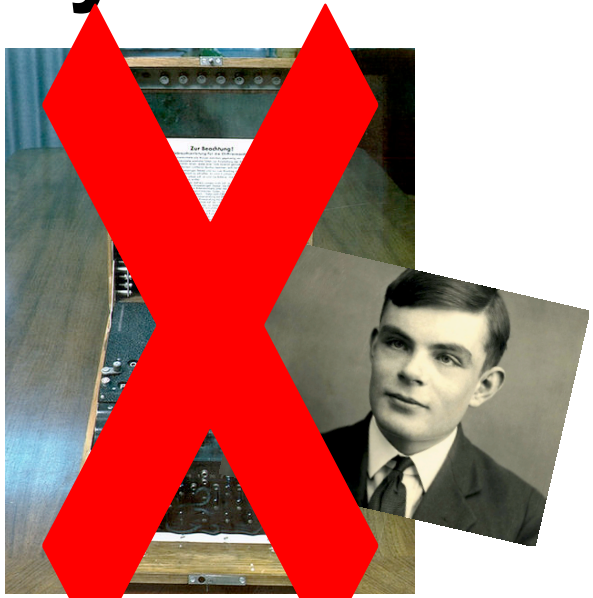
Enkel å bruke,
Små nøkler

~1940

Symmetrisk Kryptografi

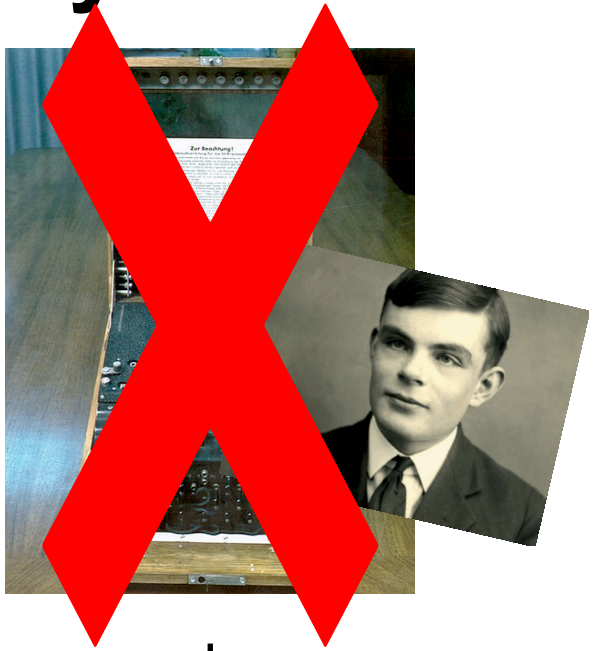
~1940

Symmetrisk Kryptografi



~1940

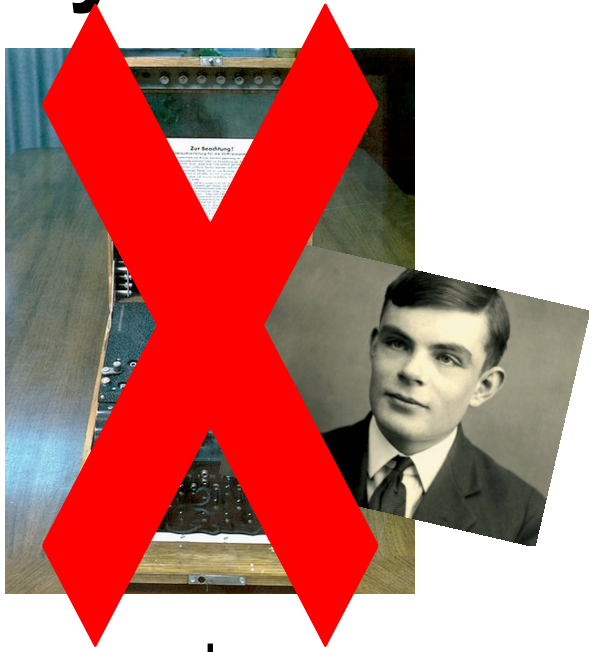
Symmetrisk Kryptografi



~1940

Kalde krigen

Symmetrisk Kryptografi

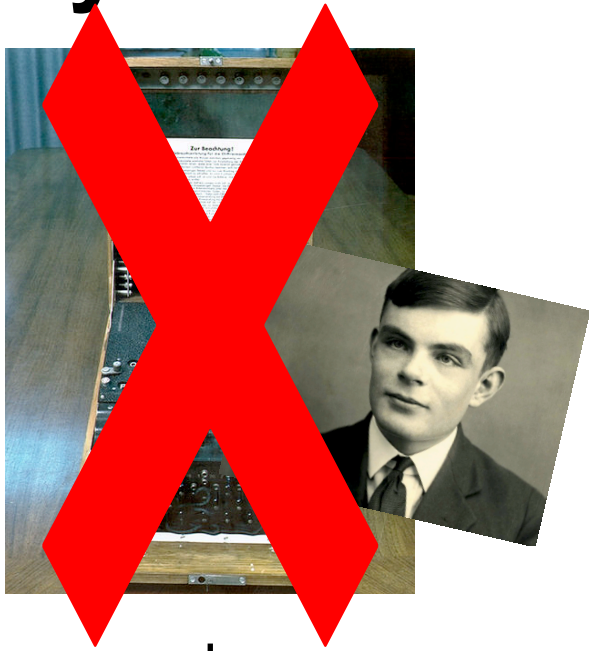


Made in

~1940

Kalde krigen

Symmetrisk Kryptografi



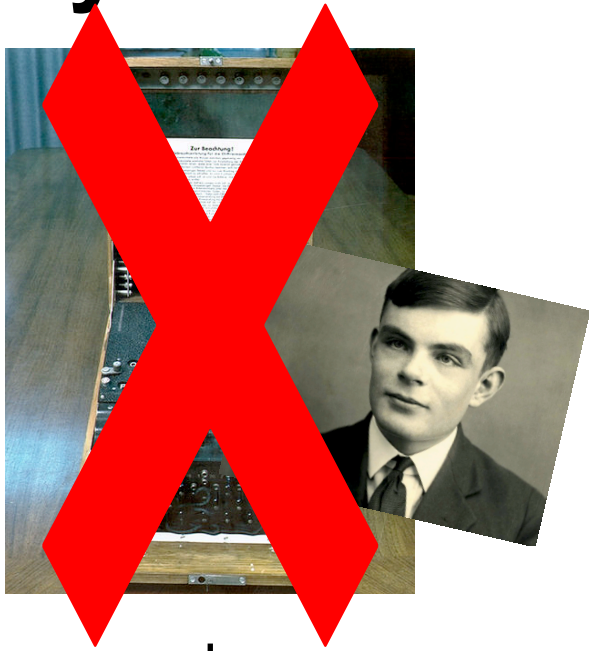
Made in

~1940

Kalde krigen

2001

Symmetrisk Kryptografi



Små, forhånds-distribuerte nøkler

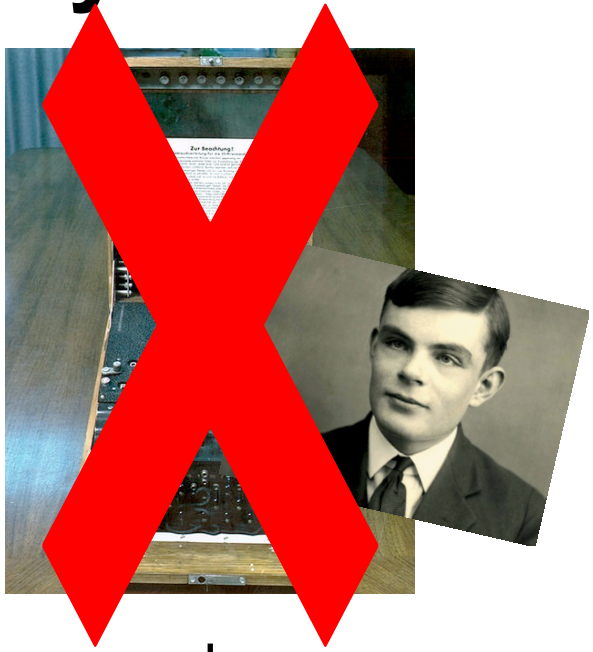
Made in

~1940

Kalde krigen

2001

Symmetrisk Kryptografi



Små, forhånds-distribuerte nøkler

Made in

~1940

Kalde krigen

2001

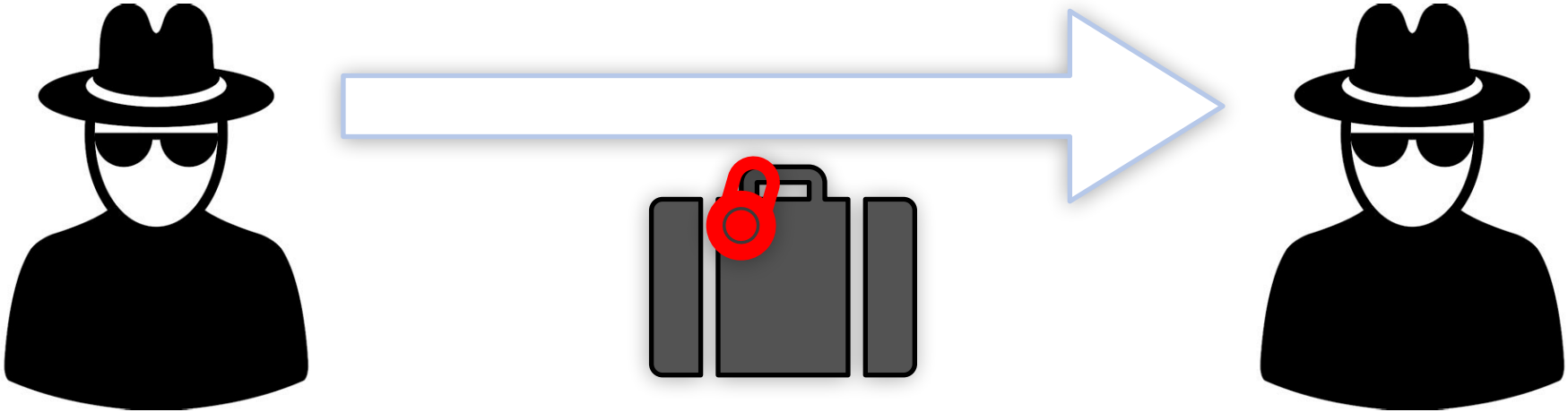
Sikker digital kommunikasjon muliggjort av matematikk!

KRYPTOGRAFI - NÅTID

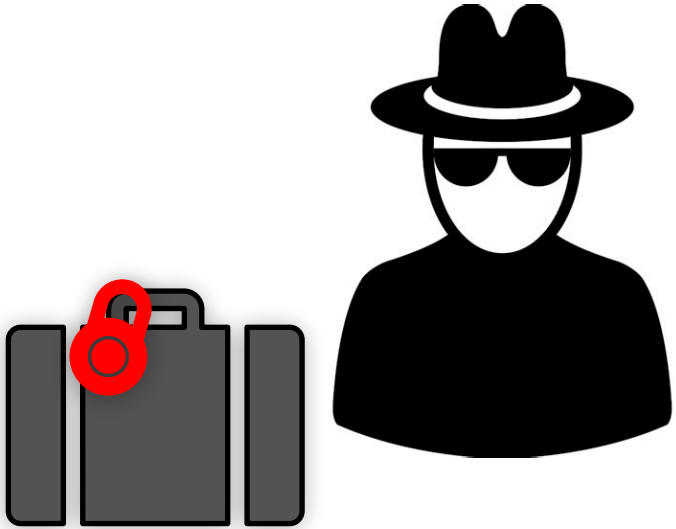
Asymmetrisk Kryptografi

Asymmetrisk Kryptografi

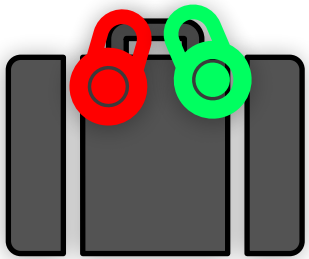
Asymmetrisk Kryptografi



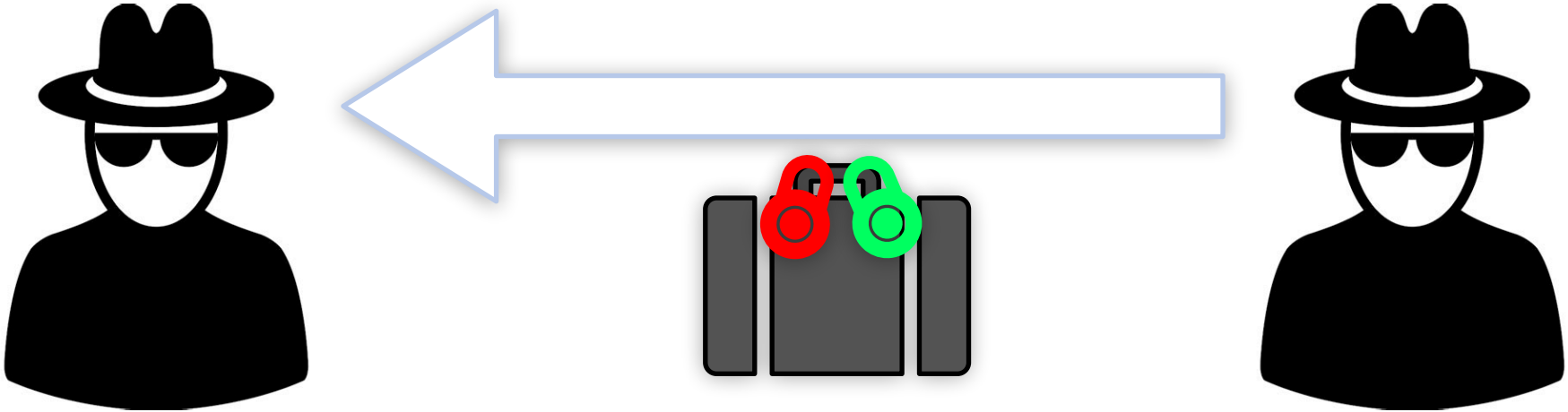
Asymmetrisk Kryptografi



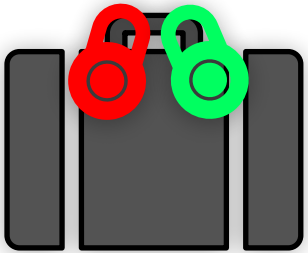
Asymmetrisk Kryptografi



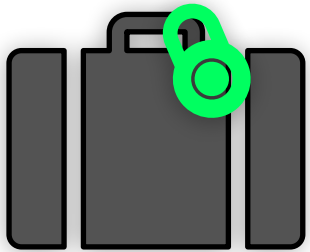
Asymmetrisk Kryptografi



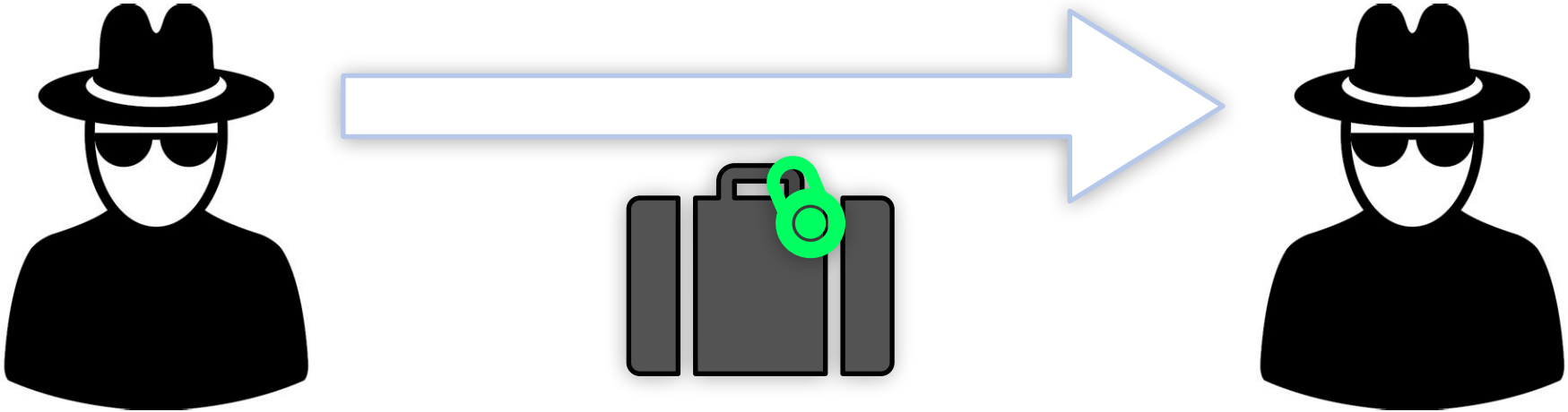
Asymmetrisk Kryptografi



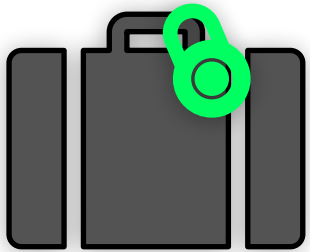
Asymmetrisk Kryptografi



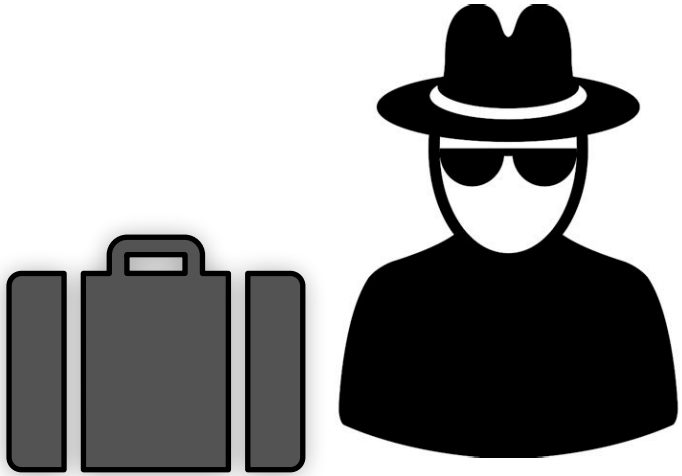
Asymmetrisk Kryptografi



Asymmetrisk Kryptografi



Asymmetrisk Kryptografi

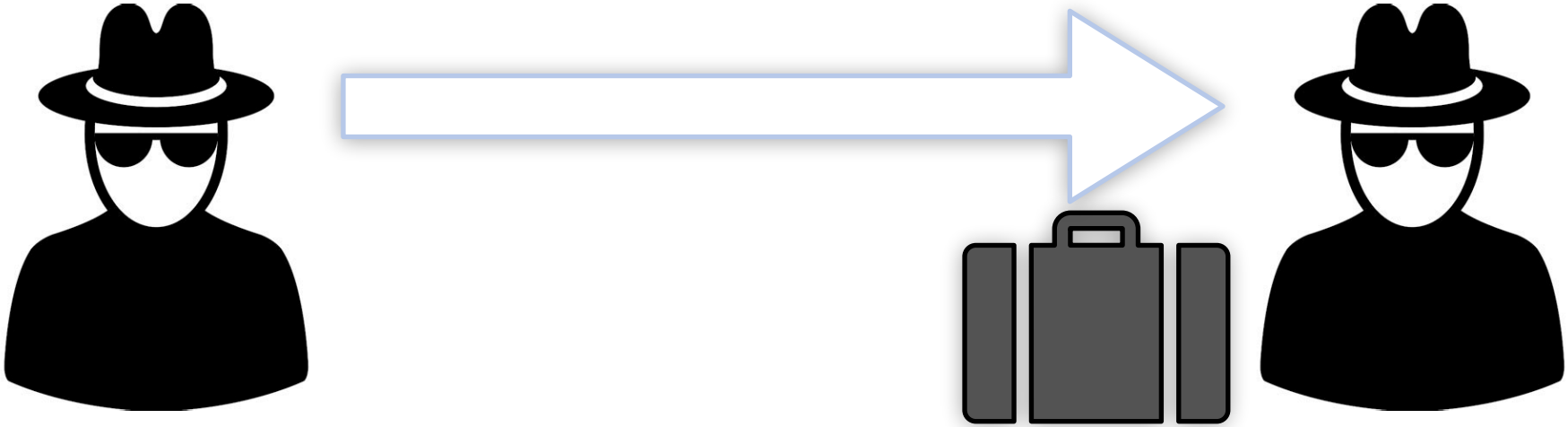


Asymmetrisk Kryptografi i virkeligheten

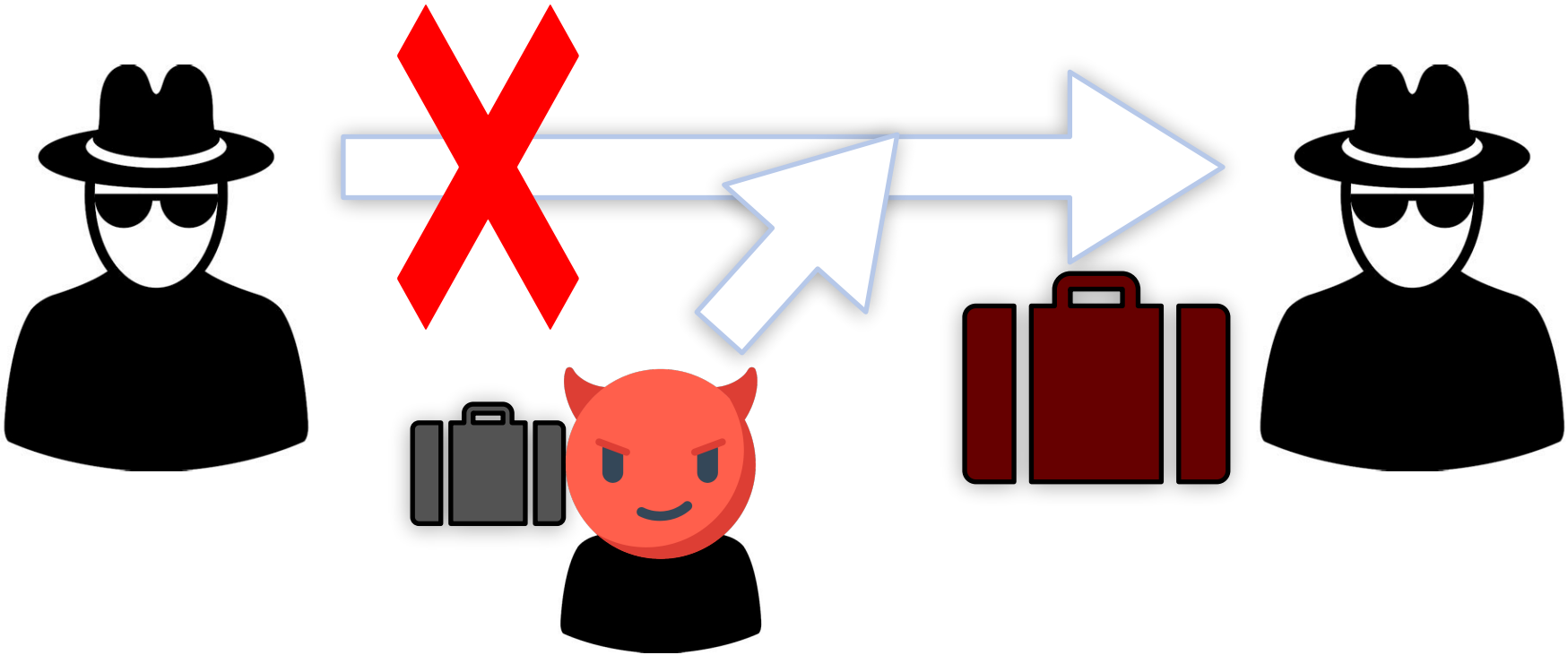
= 1 av 2 matematiske problemer

- **1. Faktorisering:**
  - **Lett:** $193 \cdot 337 = ???$
  - **Vanskelig:** $??? \cdot ??? = 65207$
- **(2. Diskret logaritmer)**

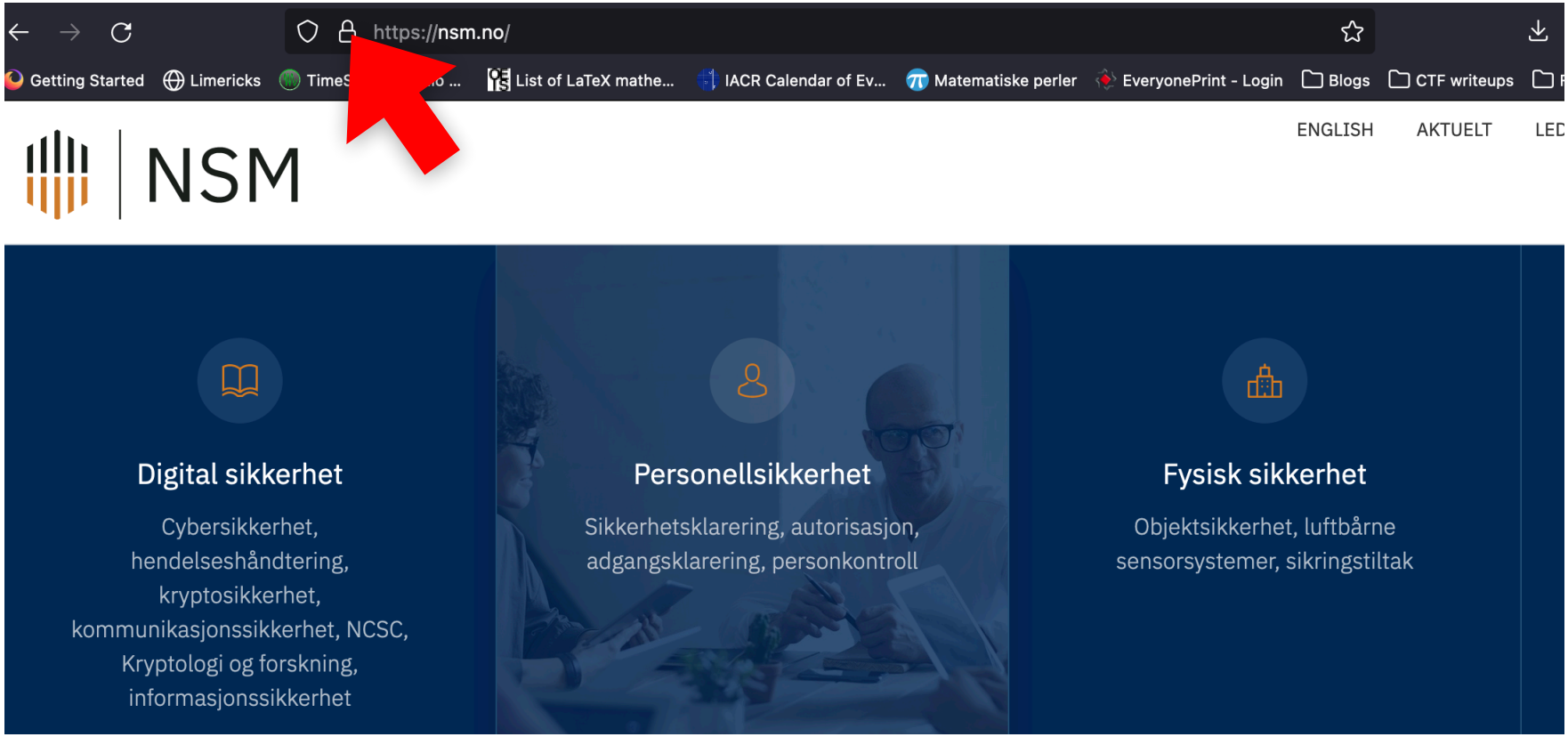
Digitale Signaturer og Meldinger



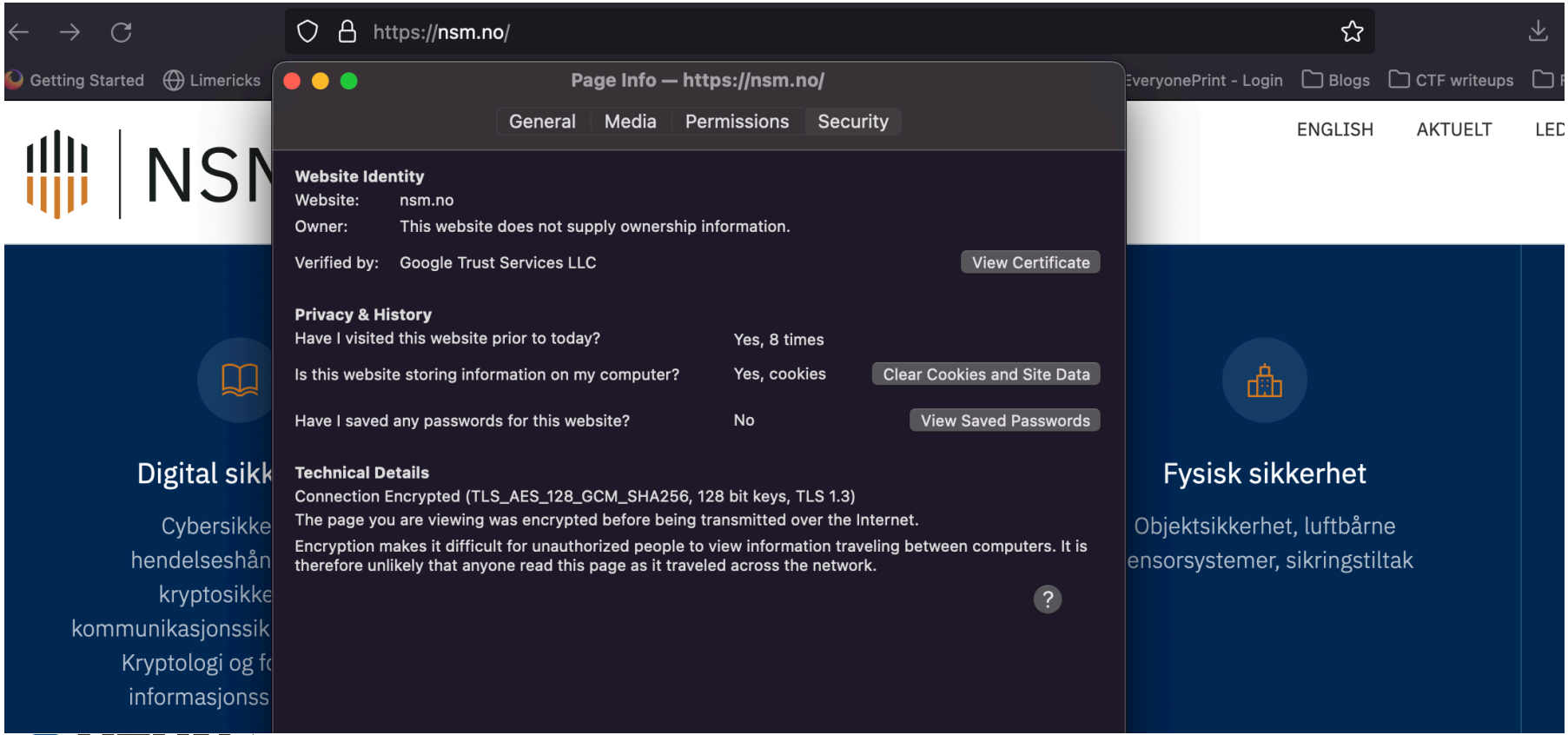
Digitale Signaturer og Meldinger



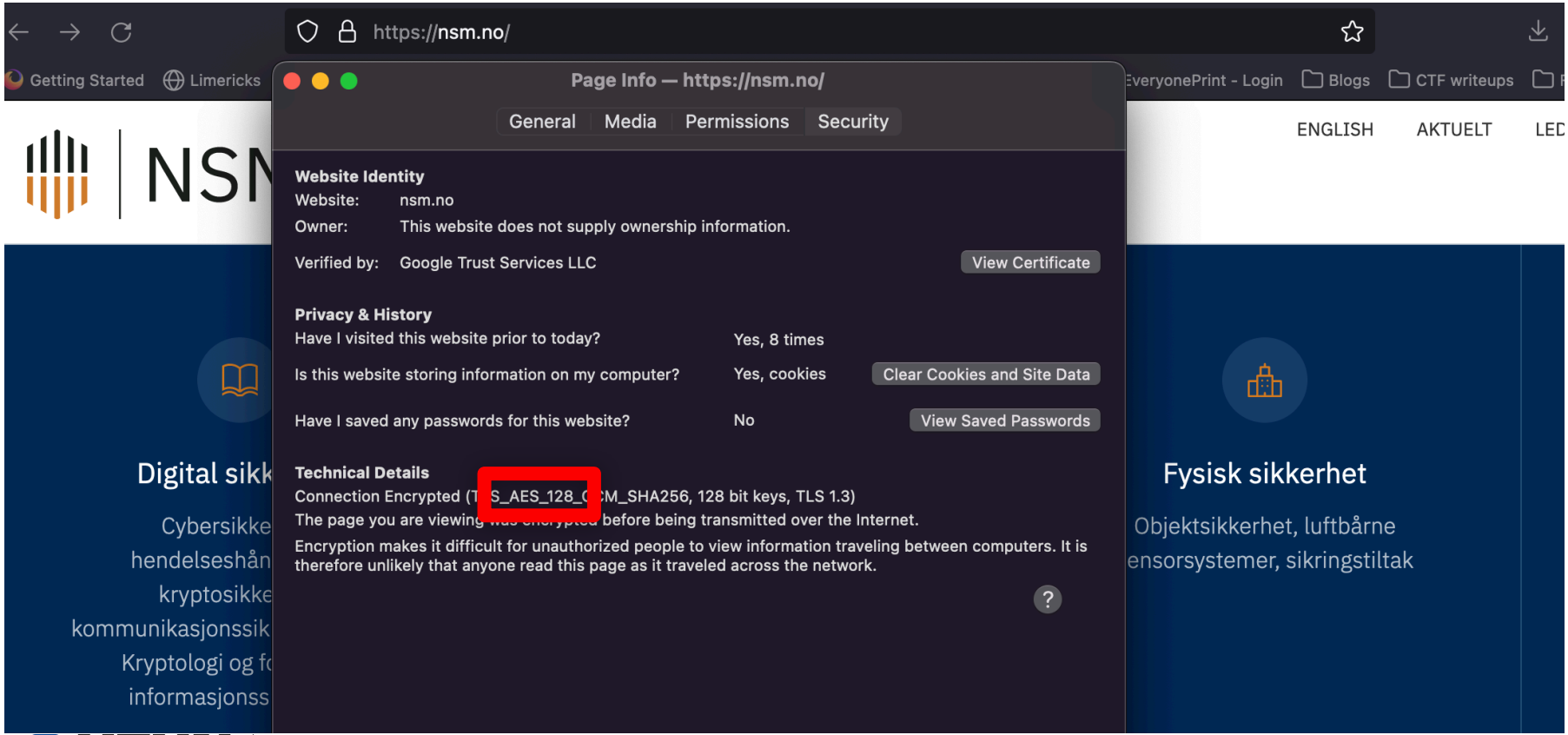
Helt essensiell del av internett



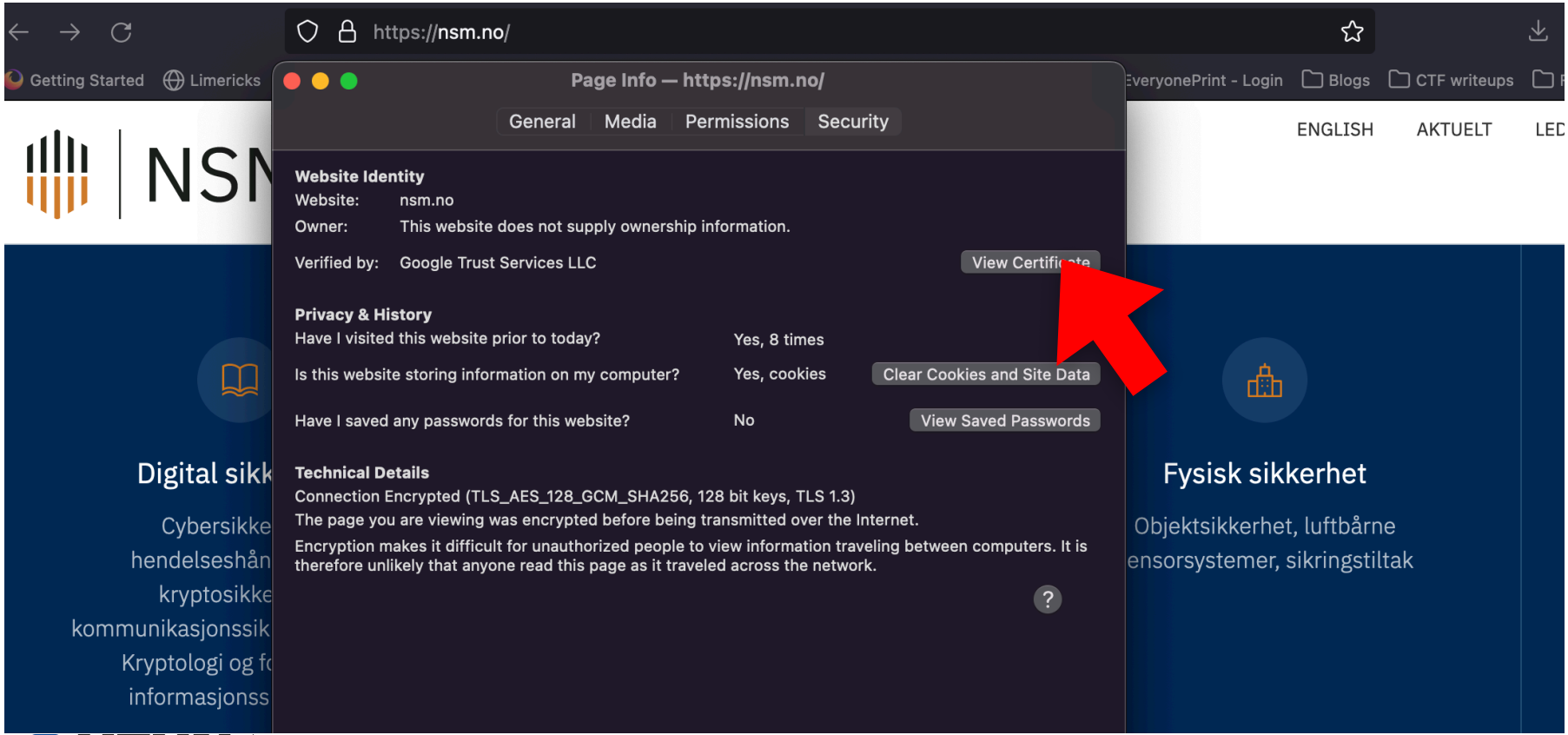
Helt essensiell del av internett



Helt essensiell del av internett



Helt essensiell del av internett



Helt essensiell del av internett

Subject Alt Names

DNS Name	nsm.no
DNS Name	*.nsm.no

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	BD:5C:29:E9:05:AE:0A:F2:4C:C5:8B:76:36:01:B5:1D:C6:84:C4:F0:E0:5E:0...

Helt essensiell del av internett

Subject Alt Names

DNS Name	nsm.no
DNS Name	*.nsm.no

Public Key Info

Kan du faktorisere dette tallet kan du utgi deg for å være *.nsm.no

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	BD:5C:29:E9:05:AE:0A:F2:4C:C5:8B:76:36:01:B5:1D:C6:84:C4:F0:E0:5E:0...

De underliggende problemene....

= 1 av 2 matematiske problemer

- **1. Faktorisering:**
  - **Lett:** $193 \cdot 337 = ???$
  - **Vanskelig:** $??? \cdot ??? = 65207$

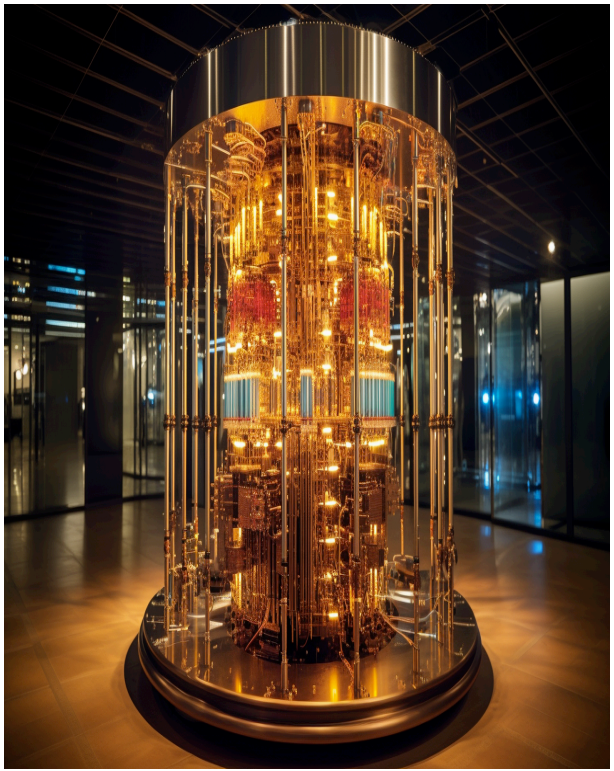
- **(2. Diskret logaritmer)**

De underliggende problemene....

= 1 av 2 matematiske problemer

- **1. Faktorisering:**
  - **Lett:** $193 \cdot 337 = ???$
  - **Lett:** $??? \cdot ??? = 65207$

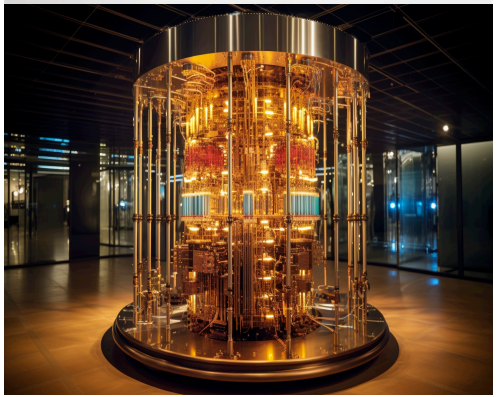
- **(2. Diskret logaritmer) (Lett)**



Kvantemaskiner???

Bits: 01110100010101000010111...

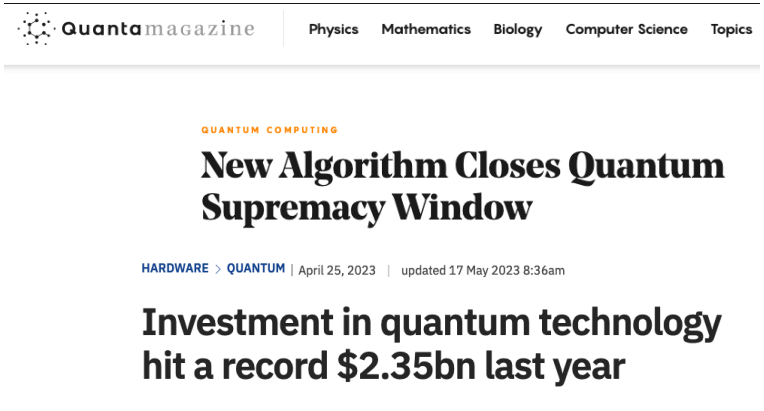
Kvantemaskiner???

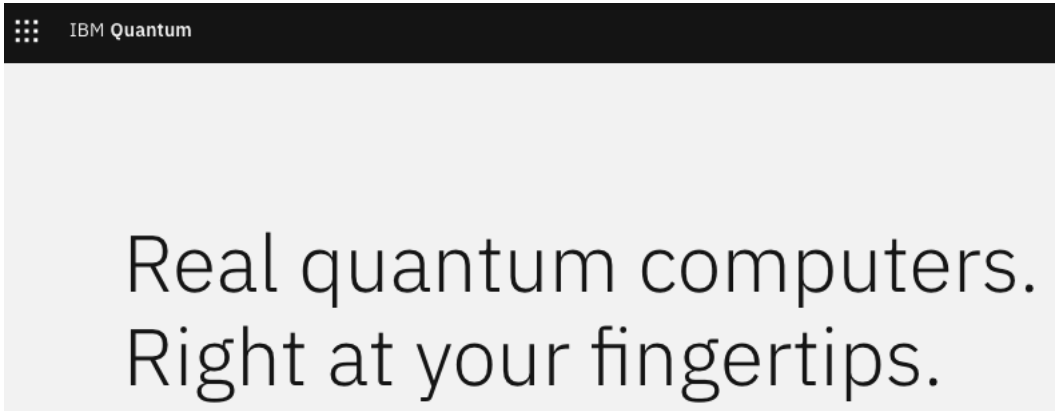


Bits: 01110100010101000010111...

Qubits: 

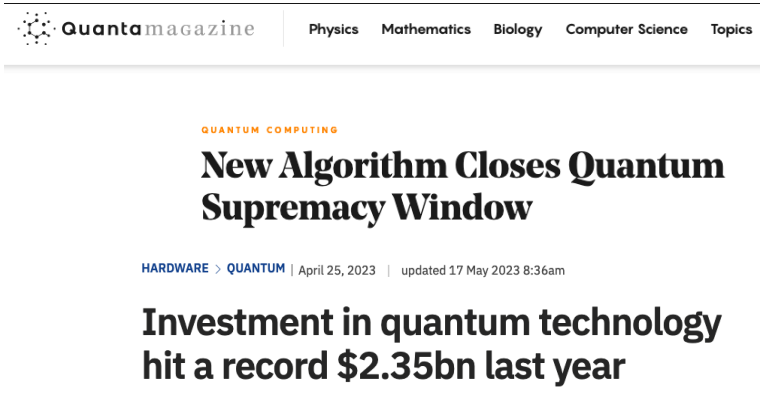
Kan kvantemaskiner bli realitet?

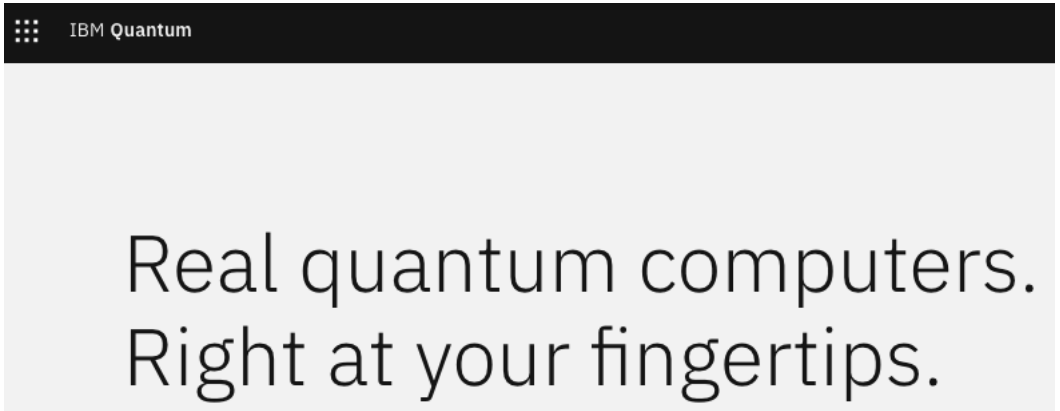




Kvantemaskiner store nok til å knekke dagens kryptografi er **5** år unna

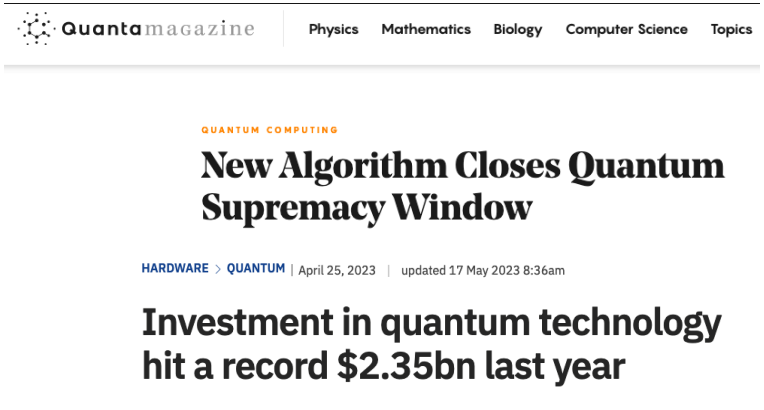
Kan kvantemaskiner bli realitet?

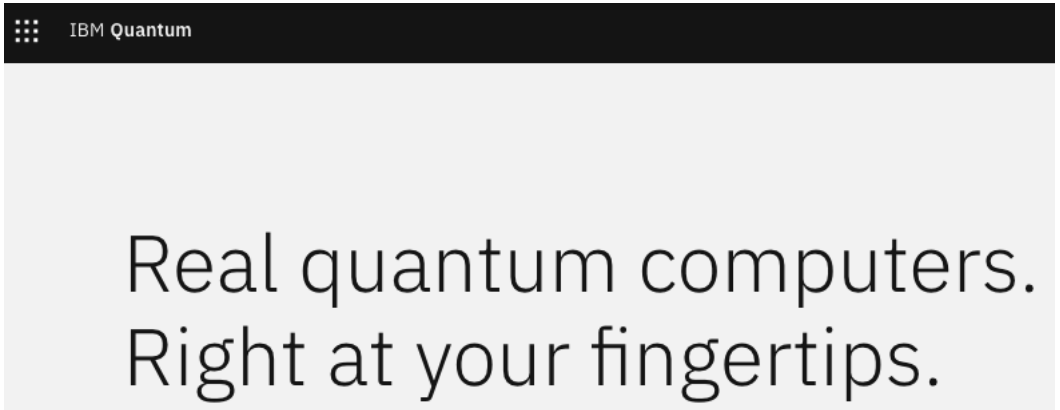




Kvantemaskiner store nok til å knekke dagens kryptografi er **30** år unna

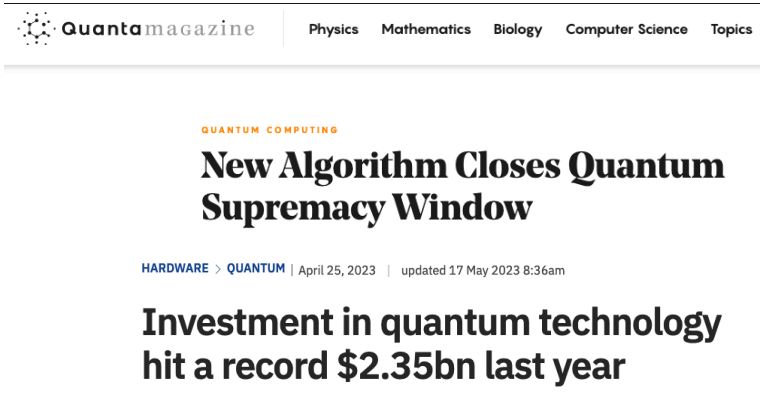
Kan kvantemaskiner bli realitet?

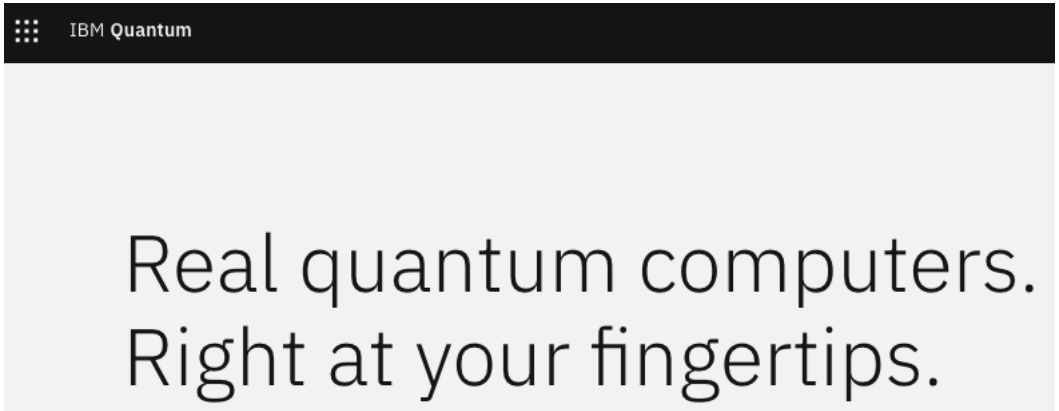




Kvantemaskiner store nok til å knekke dagens kryptografi er **0** år unna

Kan kvantemaskiner bli realitet?





Kvantemaskiner store nok til å knekke dagens kryptografi er ∞ år unna

Morgendagens kryptografi

EN KVANTESIKKER FREMTID

Kvantesikker Kryptografi

= nye matematiske problemer

- **Gitter (Latticer) ?**
- **Isogenier !?**
- **Feil-korrigerende koder ?!**
- **Flervariable ligninger ??**
- **....**

Nye standarder på vei!

NIST
National Institute of Standards and Technology

Kvantesikker Kryptografi

= nye matematiske problemer

- **Gitter (Latticer) ?**
- **Isogenier !?**
- **Feil-korrigerende koder ?!**
- **Flervariable ligninger ??**
- **....**

Nye standarder på vei!

Not an International STandard

Kvantesikker Kryptografi

= nye matematiske problemer

- **Gitter (Latticer) ?**
- **Isogenier !?**
- **Feil-korrigerende koder ?!**
- **Flervariable ligninger ??**
- **....**

Nye standarder på vei!

Not an International STandard

NSM

UPDATES

NIST Announces Additional Digital Signature Candidates for the PQC Standardization Process

NIST has completed the reviews for all the "onramp" digital signature submissions received by the deadline.

July 17, 2023

Når må man over på ny kryptografi?

- **X** = Antall år konfidensiell informasjon må holdes hemmelig

Når må man over på ny kryptografi?

- **X** = Antall år konfidensiell informasjon må holdes hemmelig
- **Y** = Antall år før kvantesikker krypto kan integreres i systemet ditt

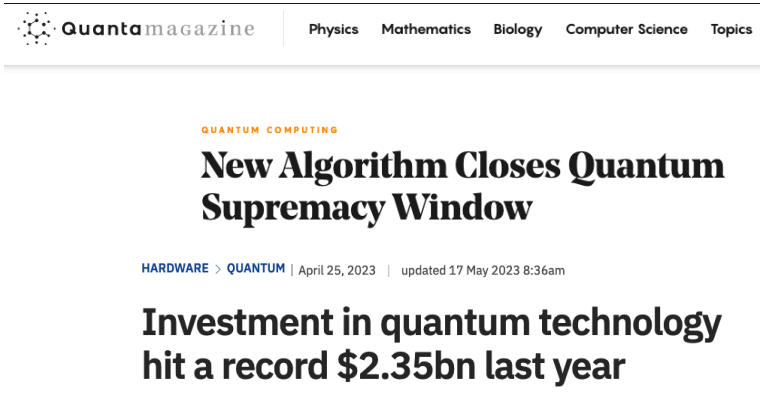
Når må man over på ny kryptografi?

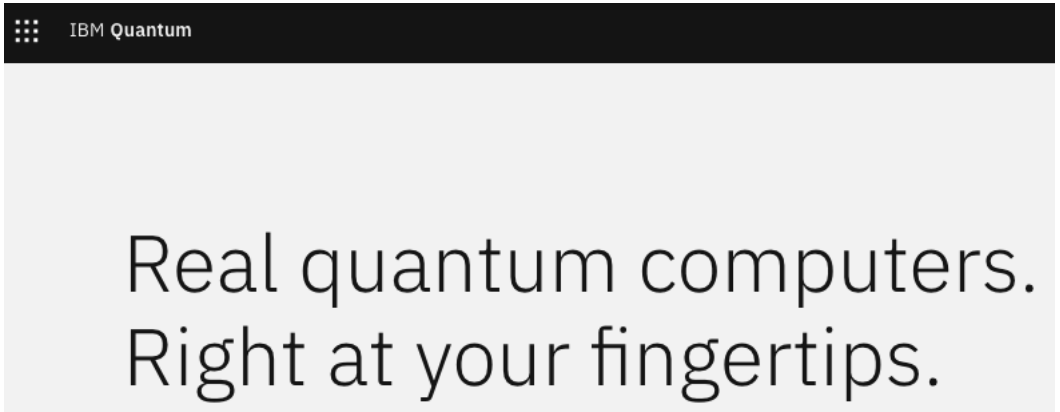
- **X** = Antall år konfidensiell informasjon må holdes hemmelig
- **Y** = Antall år før kvantesikker krypto kan integreres i systemet ditt
- **Z** = Antall år før en fullskala kvantemaskin finnes

Når må man over på ny kryptografi?

- **X** = Antall år konfidensiell informasjon må holdes hemmelig
- **Y** = Antall år før kvantesikker krypto kan integreres i systemet ditt
- **Z** = Antall år før en fullskala kvantemaskin finnes
- **Teorem (Moscha):**
  Hvis X + Y > Z er det på tide å bli bekymret!

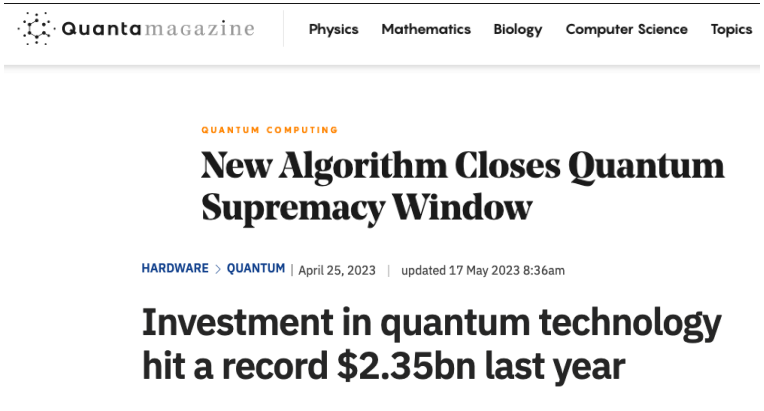
Hva om kvantemaskiner aldri kommer?

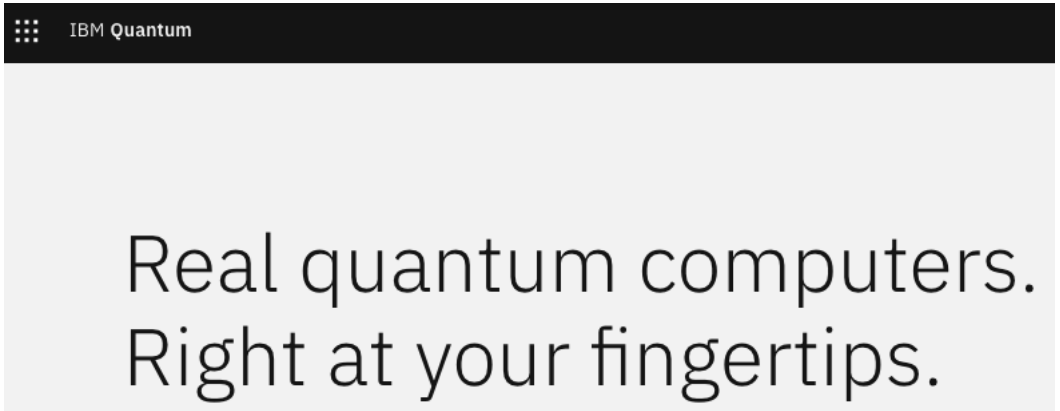




Kvantemaskiner store nok til å knekke dagens kryptografi er ∞ år unna

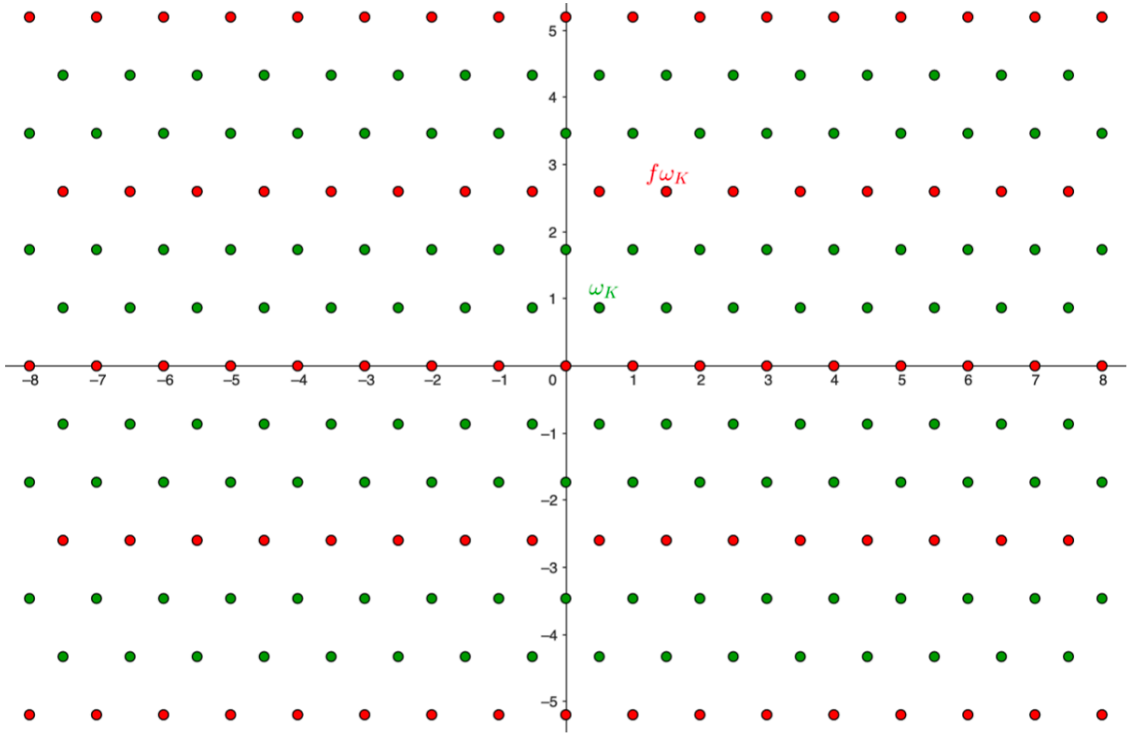
Hva om kvantemaskiner aldri kommer?





Kvantemaskiner store nok til å knekke dagens kryptografi er ∞ år unna

Spiller ingen rolle, alle må over på nye standarder etterhvert



Tusen takk!

Epost: jonathan.k.eriksen@ntnu.no
Nettside: jonathke.github.io