



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:

 Nyheter Sport Kultur Humor Distrikt Mer ▾

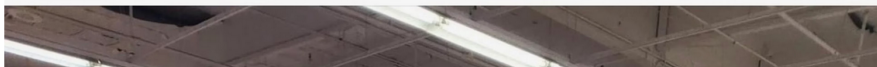
Logg på

Norge Siste nytt Dokumentar Klima NRK Ytring

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

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

 Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... [Se mer](#)



 [Snorre Tønset](#)
Journalist



Historisk: Bok-Chiffer

Melding: **A**ngrip imorgen

Chiffertekst: 2/8

 **Nyheter** Sport Kultur Humor Distrikt Mer ▾

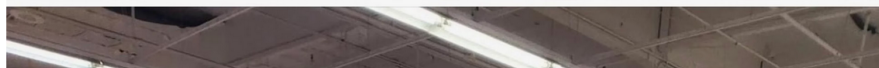
Logg på 🔍 Sø

Norge Siste nytt Dokumentar Klima NRK Ytring

Nettsvindel øker kraftig: Advarer mot å trykke på slike **a**annonser

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

 Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... [Se mer](#)



 [Snorre Tønset](#)
Journalist



Historisk: Bok-Chiffer

Melding: **A**ngrip imorgen

Chiffertekst: 2/8, 1/1

 **Nyheter** Sport Kultur Humor Distrikt Mer ▾

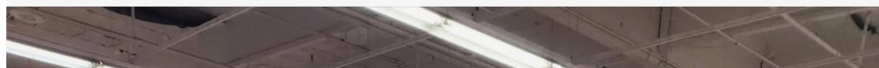
Logg på 🔍 Sø

Norge Siste nytt Dokumentar Klima NRK Ytring

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

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

 Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... [Se mer](#)



 [Snorre Tønset](#)
Journalist



Historisk: Bok-Chiffer

Melding: Angrip imorgen

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

 Nyheter Sport Kultur Humor Distrikt Mer ▾

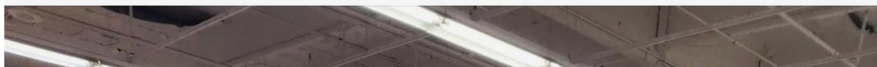
Logg på 🔍 Sø

Norge Siste nytt Dokumentar Klima NRK Ytring

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

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

 Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... Se mer



✉ Snorre Tønset
Journalist



Historisk: Bok-Chiffer

Melding: Angrip imorgen

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

 **NRK**

[Nyheter](#) [Sport](#) [Kultur](#) [Humor](#) [Distrikt](#) [Mer](#) 

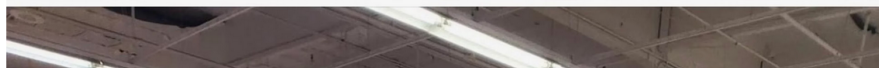
 Logg på  Sø

[Norge](#) [Siste nytt](#) [Dokumentar](#) [Klima](#) [NRK Ytring](#)

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

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

 Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... [Se mer](#)



 [Snorre Tønset](#)
Journalist



Historisk: Bok-Chiffer

Melding: Angrip imorgen

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

 **Nyheter** Sport Kultur Humor Distrikt Mer ▾

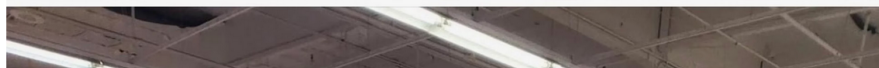
 Logg på  Sø

Norge Siste nytt Dokumentar Klima NRK Ytring

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

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

 Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... [Se mer](#)



 [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.

 Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... [Se mer](#)



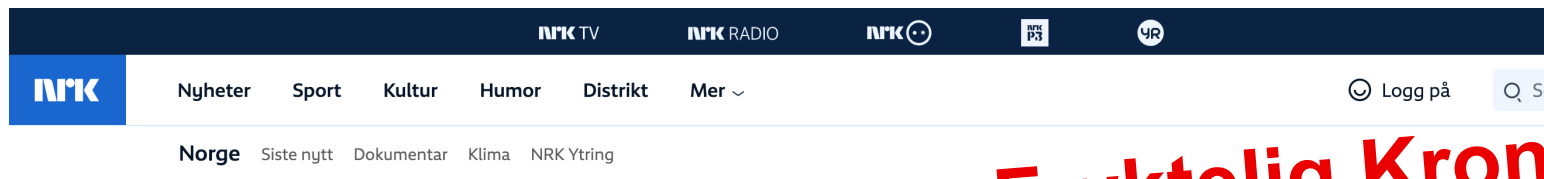
 [Snorre Tønset](#)
Journalist



Historisk: Bok-Chiffer

Melding: Angrip imorgen

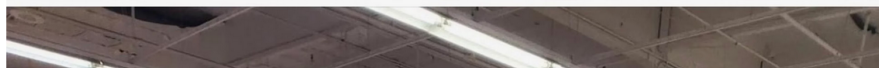
Chiffertekst: 2/8, 1/1, 1/22, 3/7, ...



Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

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

 Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... Se mer



Fryktelig Kronglete
Store, vanskelig å distribuere, nøkler



 Snorre Tønset
Journalist

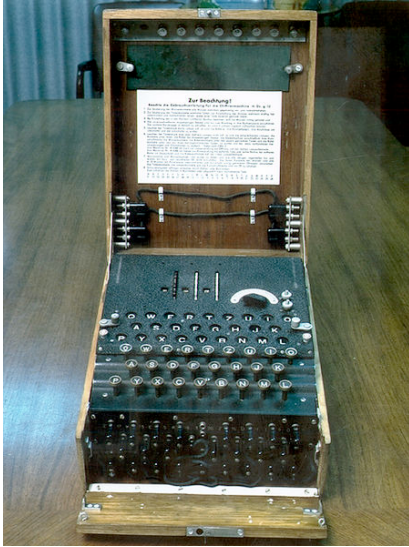


Symmetrisk Kryptografi



~1940

Symmetrisk Kryptografi



Enkel å bruke,
Små nøkler

~1940



NTNU

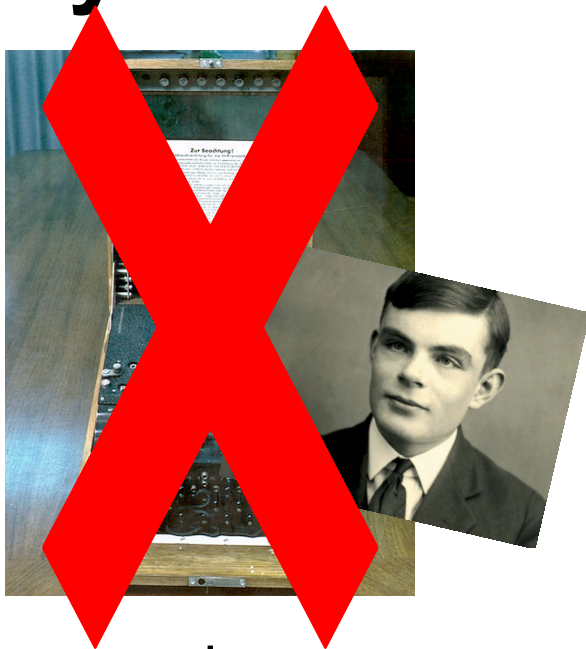
Kunnskap for en bedre verden

Symmetrisk Kryptografi



~1940

Symmetrisk Kryptografi



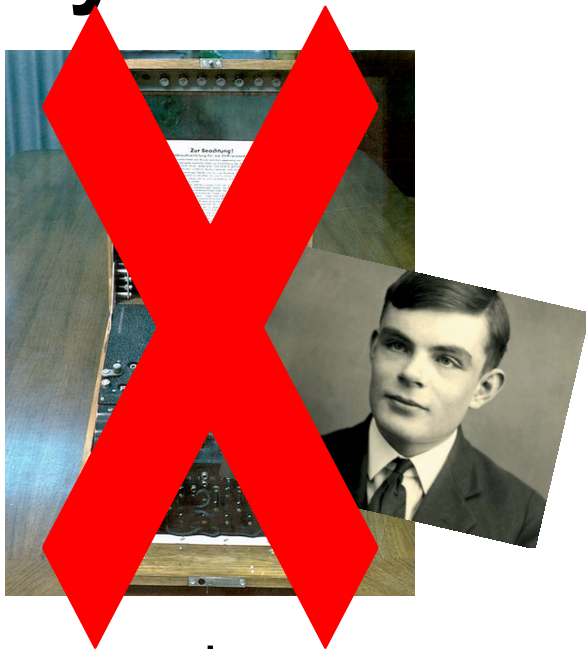
~1940



NTNU

Kunnskap for en bedre verden

Symmetrisk Kryptografi



~1940



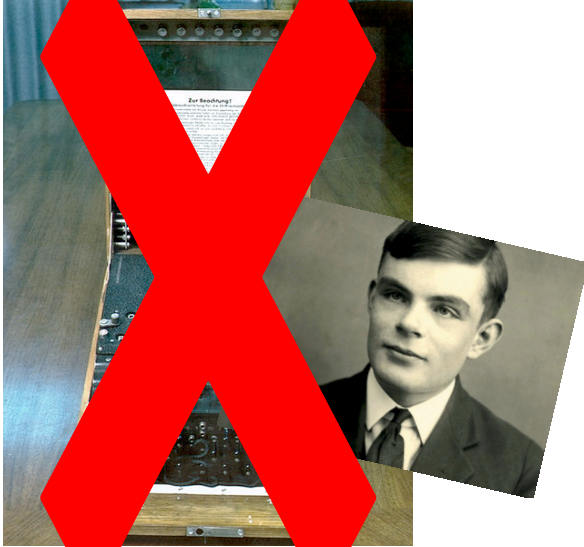
Kalde krigen



NTNU

Kunnskap for en bedre verden

Symmetrisk Kryptografi



~1940

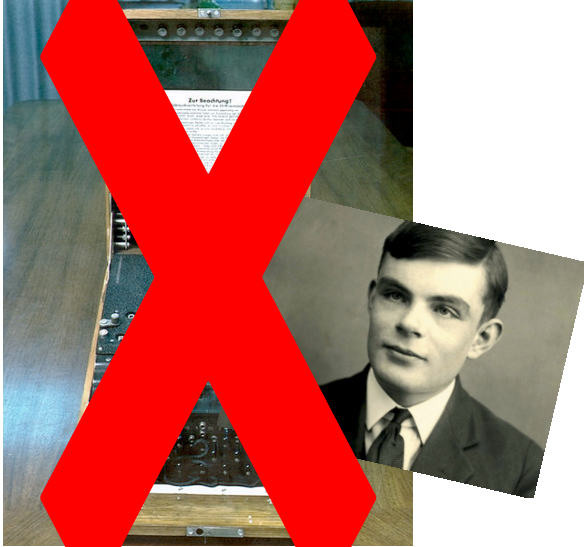


Made in



Kalde krigen

Symmetrisk Kryptografi



~1940



Made in

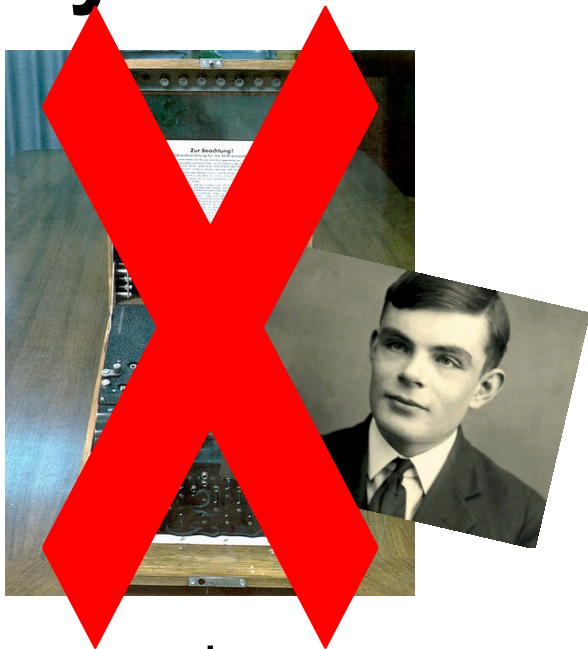


Kalde krigen



2001

Symmetrisk Kryptografi



~1940



Made in



Kalde krigen

Små, forhånds-
distribuerte nøkler



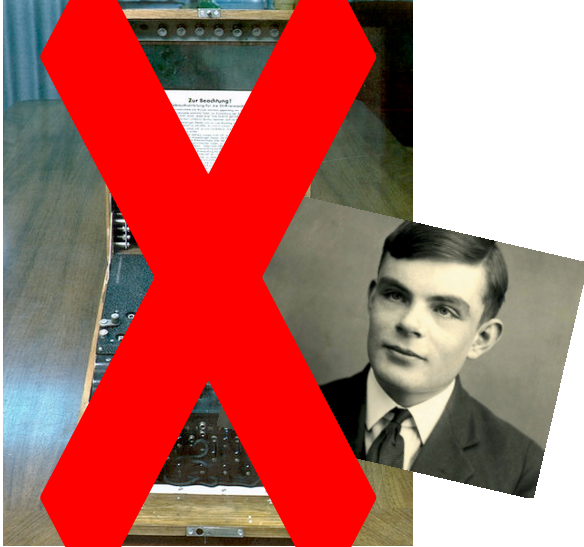
2001



NTNU

Kunnskap for en bedre verden

Symmetrisk Kryptografi



~1940



Made in



Kalde krigen

Små, forhånds-
distribuerte nøkler



2001

Sikker digital kommunikasjon muliggjort av matematikk!

KRYPTOGRAFI - NÅTID

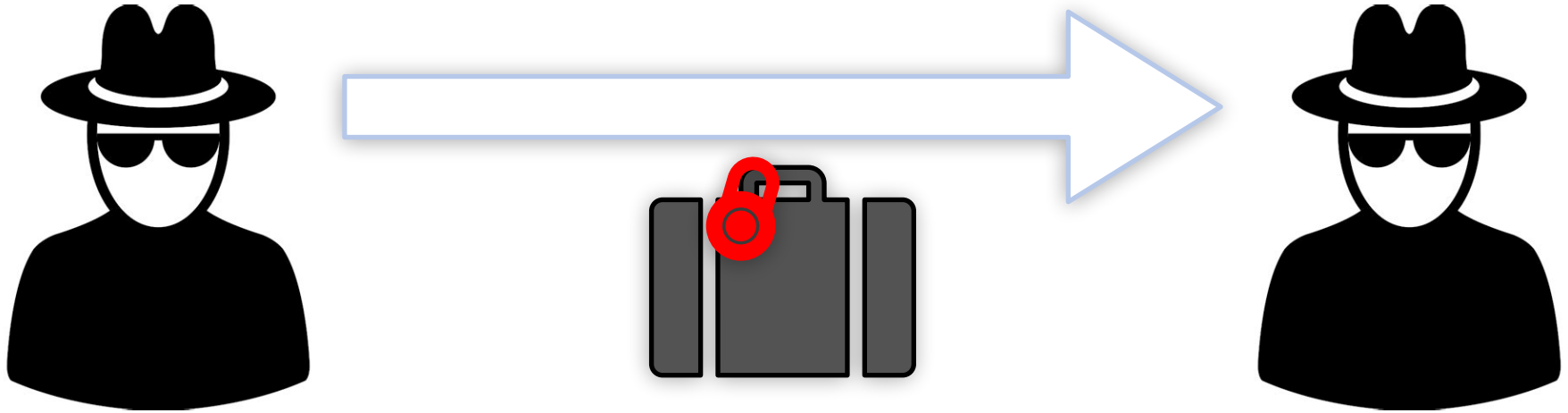
Asymmetrisk Kryptografi



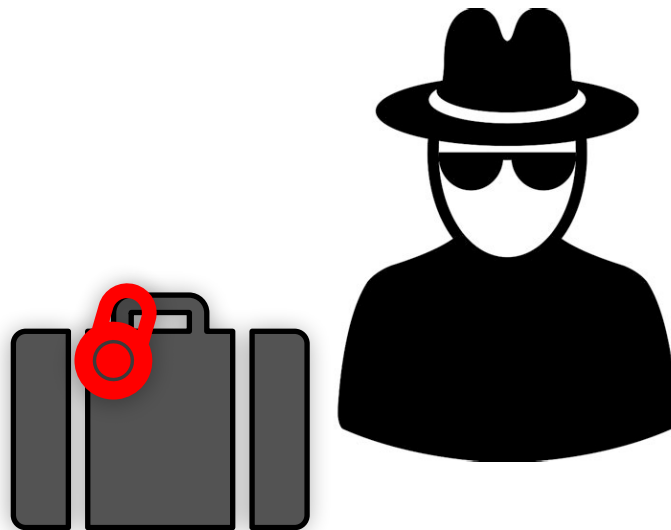
Asymmetrisk Kryptografi



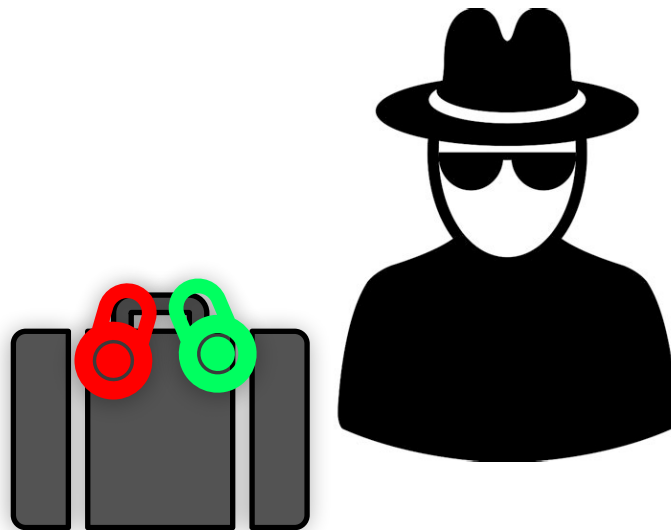
Asymmetrisk Kryptografi



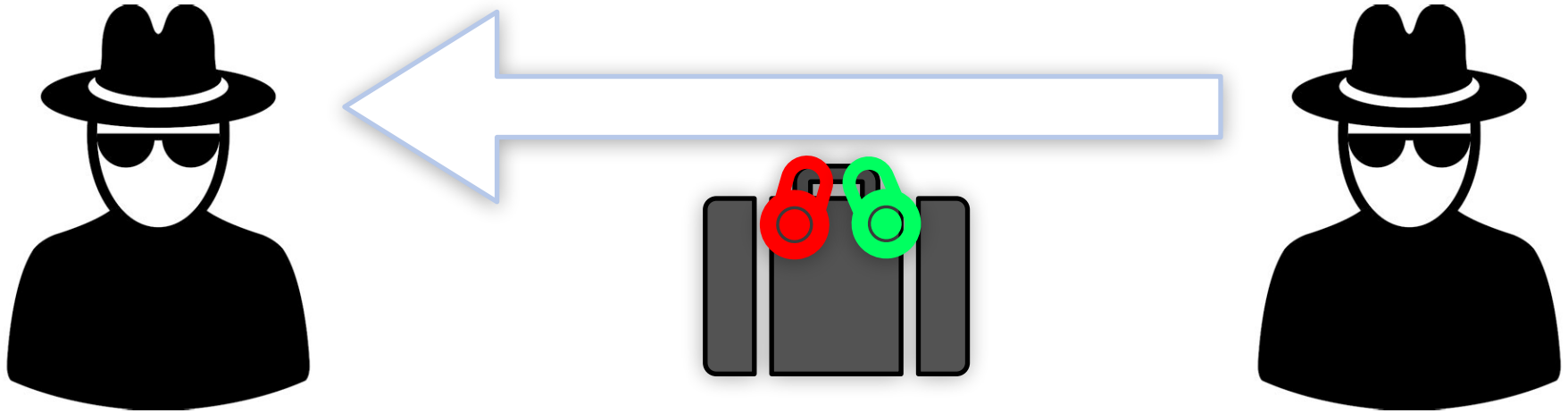
Asymmetrisk Kryptografi



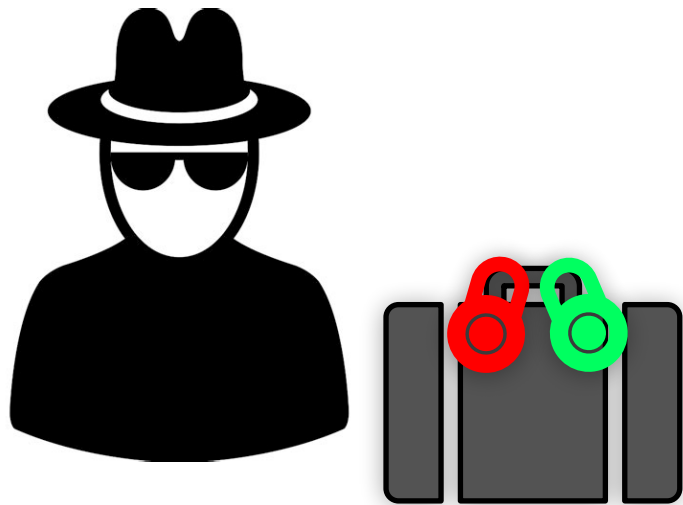
Asymmetrisk Kryptografi



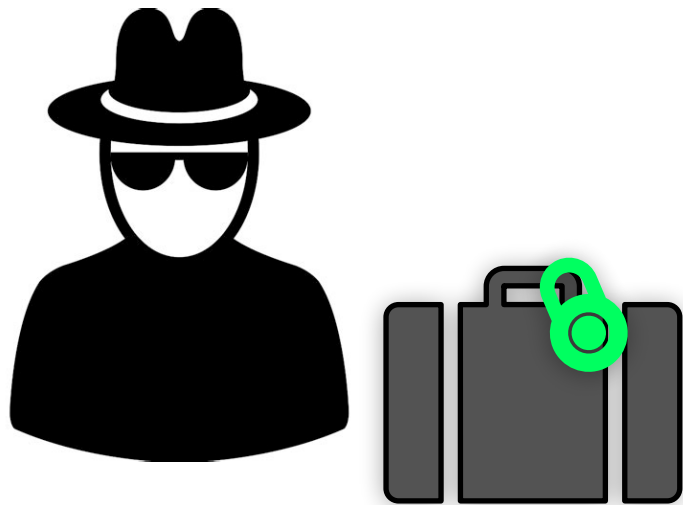
Asymmetrisk Kryptografi



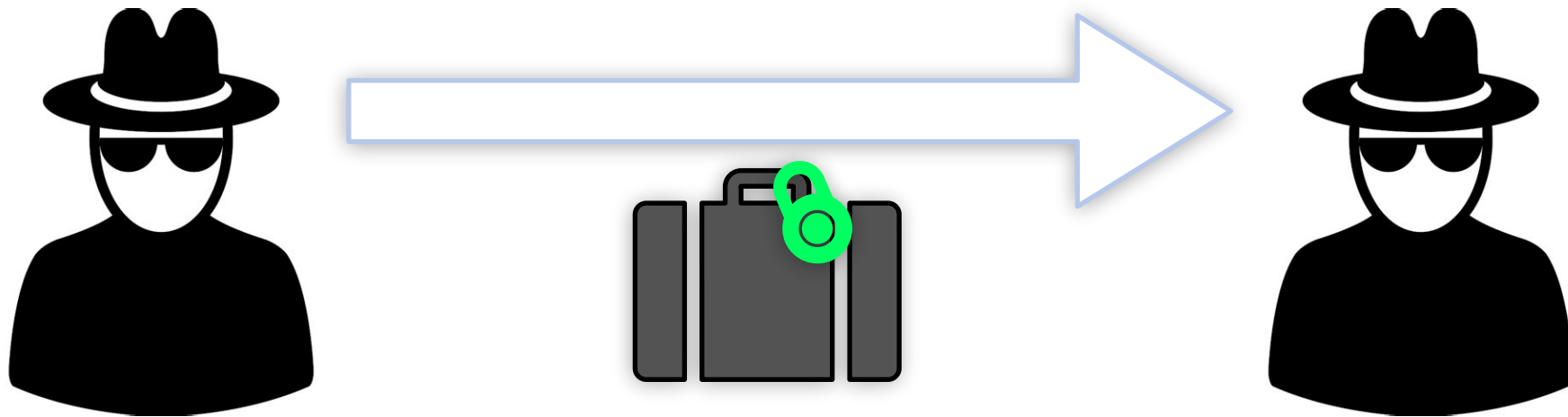
Asymmetrisk Kryptografi



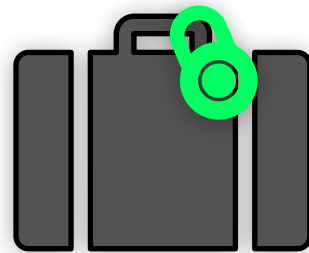
Asymmetrisk Kryptografi



Asymmetrisk Kryptografi



Asymmetrisk Kryptografi



Asymmetrisk Kryptografi



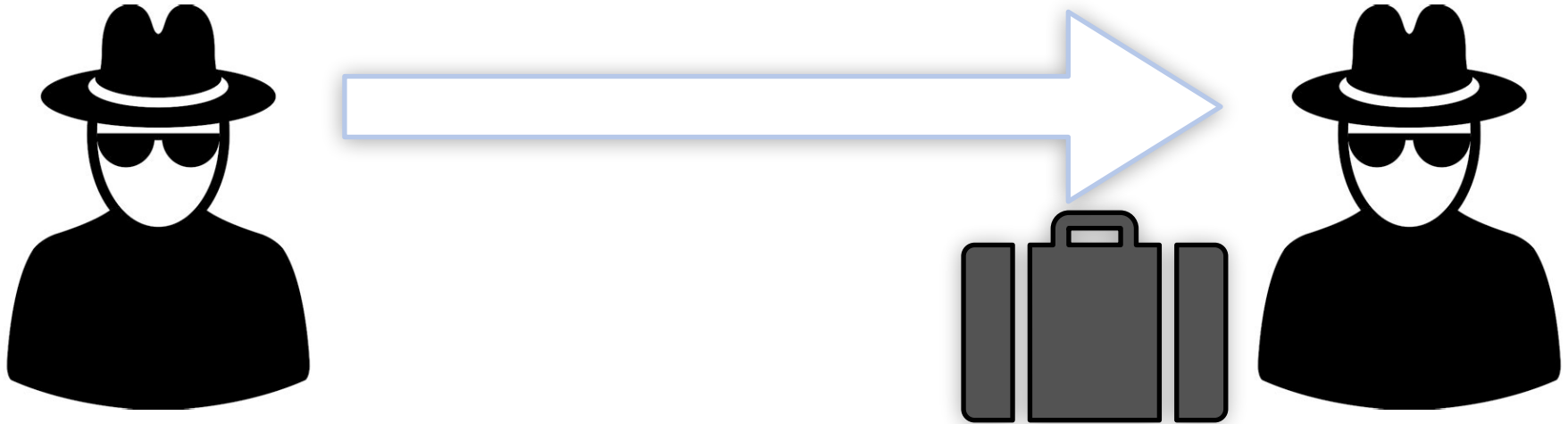
Asymmetrisk Kryptografi i virkeligheten



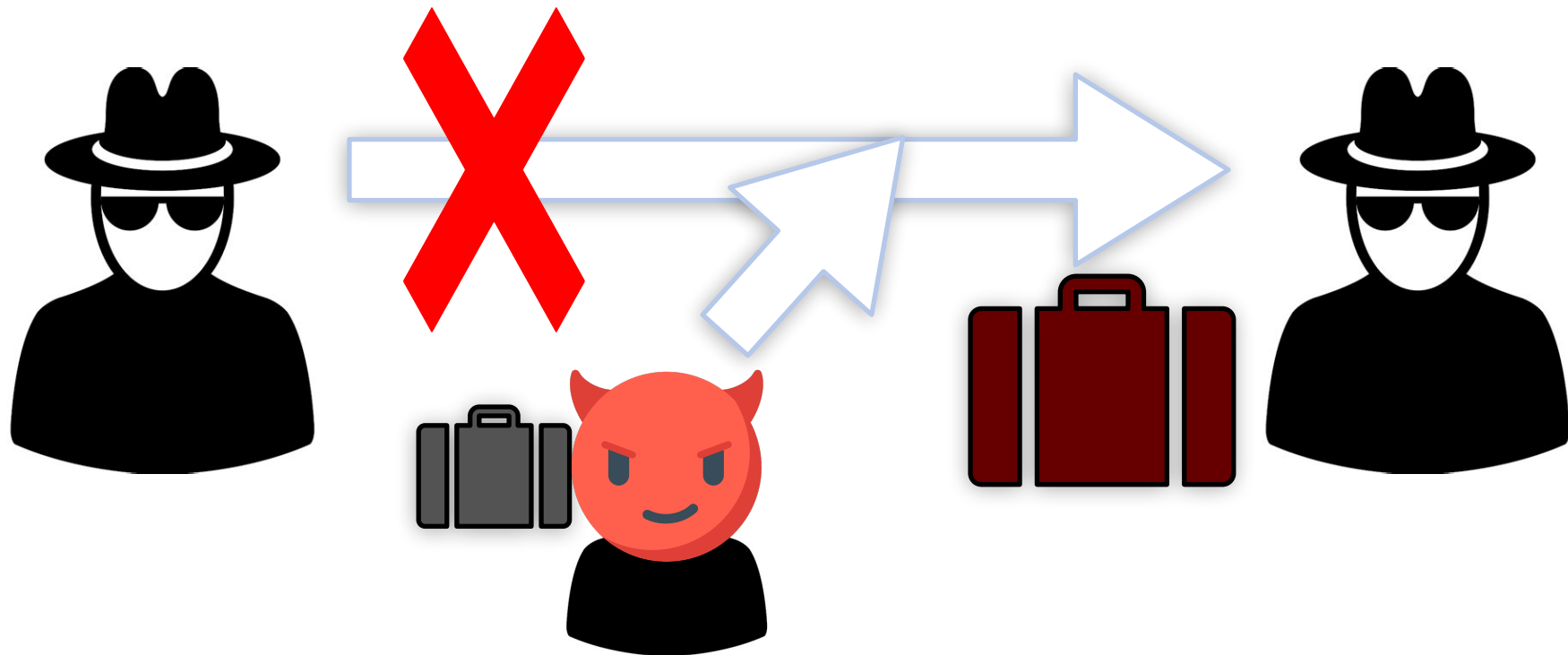
= 1 av 2 matematiske problemer

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

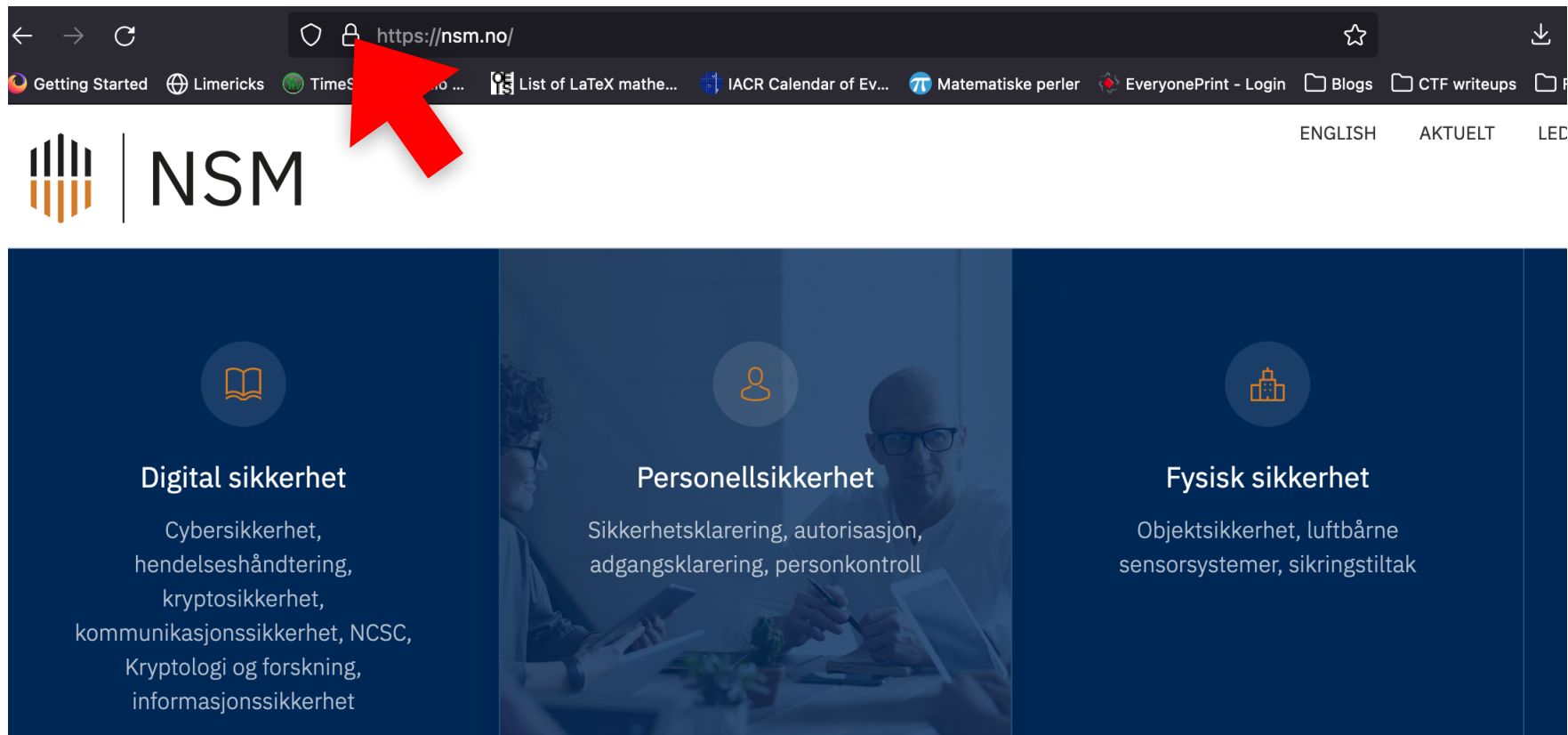
Digitale Signaturer og Meldinger



Digitale Signaturer og Meldinger



Helt essensiell del av internett



← → ↻ <https://nsm.no/> ☆ ⌵

Getting Started Limericks Times no ... List of LaTeX mathe... IACR Calendar of Ev... Matematiske perler EveryonePrint - Login Blogs CTF writeups P

 | NSM ENGLISH AKTUELT LEC



Digital sikkerhet

Cybersikkerhet,
hendelseshåndtering,
kryptosikkerhet,
kommunikasjonssikkerhet, NCSC,
Kryptologi og forskning,
informasjonssikkerhet



Personellsikkerhet

Sikkerhetsklarering, autorisasjon,
adgangsklarering, personkontroll



Fysisk sikkerhet

Objektsikkerhet, luftbårne
sensorsystemer, sikringstiltak



NTNU

Kunnskap for en bedre verden

Helt essensiell del av internett

The screenshot shows a web browser window with the address bar displaying `https://nsm.no/`. The browser's address bar includes navigation buttons (back, forward, refresh), a security icon (lock), and a star icon for bookmarks. The page title is "Page Info — https://nsm.no/". The "Page Info" window is open, showing the following information:

- General** (selected tab)
- Website Identity**
 - Website: `nsm.no`
 - Owner: This website does not supply ownership information.
 - Verified by: Google Trust Services LLC [View Certificate](#)
- Privacy & History**
 - Have I visited this website prior to today? Yes, 8 times
 - Is this website storing information on my computer? Yes, cookies [Clear Cookies and Site Data](#)
 - Have I saved any passwords for this website? No [View Saved Passwords](#)
- Technical Details**
 - Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
 - The page you are viewing was encrypted before being transmitted over the Internet.
 - Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

The background shows the NSM website with a dark blue header and a main content area. The header includes the NSM logo and navigation links: "Getting Started", "Limericks", "EveryonePrint - Login", "Blogs", "CTF writeups", and "F". The main content area has a large blue section with the text "Digital sikkerhet" and "Cybersikkerhet, hendelseshåndtering, kryptosikkerhet, kommunikasjonssikkerhet, Kryptologi og fysisk informasjonssikkerhet". To the right, there is a section titled "Fysisk sikkerhet" with the text "Objektsikkerhet, luftbårne sensorsystemer, sikringstiltak".

Helt essensiell del av internett

The screenshot shows a web browser displaying the NSM (Norwegian Security Monitor) website. A 'Page Info' window is open, showing details for the URL <https://nsm.no/>. The 'Technical Details' section is highlighted with a red box, indicating the connection is encrypted using TLS 1.3 with AES-128-GCM and SHA256. The background of the browser shows the NSM website with a dark blue header and a sidebar on the left containing the text 'Digital sikkerhet' and 'Cybersikkerhet'. The main content area on the right is titled 'Fysisk sikkerhet' and lists 'Objektsikkerhet, luftbårne sensorsystemer, sikringstiltak'.

Getting Started Limericks

Page Info — <https://nsm.no/>

General Media Permissions Security

Website Identity

Website: nsm.no

Owner: This website does not supply ownership information.

Verified by: Google Trust Services LLC [View Certificate](#)

Privacy & History

Have I visited this website prior to today? Yes, 8 times

Is this website storing information on my computer? Yes, cookies [Clear Cookies and Site Data](#)

Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

?

ENGLISH AKTUELT LEC

Digital sikkerhet

Cybersikkerhet

hendelseshåndtering

kryptosikkerhet

kommunikasjonssikkerhet

Kryptologi og forebyggelse

informasjonssikkerhet

Fysisk sikkerhet

Objektsikkerhet, luftbårne sensorsystemer, sikringstiltak

Helt essensiell del av internett

The screenshot shows a web browser window with the address bar displaying `https://nsm.no/`. The browser's address bar includes navigation buttons (back, forward, refresh) and a star icon for bookmarks. The page content is partially visible, showing the NSM logo and navigation links like 'Getting Started', 'Limericks', 'EveryonePrint - Login', 'Blogs', 'CTF writeups', 'ENGLISH', 'AKTUELT', and 'LEC'. A 'Page Info' dialog box is open, showing the 'Security' tab. The dialog box contains the following information:

- Website Identity**
 - Website: nsm.no
 - Owner: This website does not supply ownership information.
 - Verified by: Google Trust Services LLC
 - [View Certificate](#)
- Privacy & History**
 - Have I visited this website prior to today? Yes, 8 times
 - Is this website storing information on my computer? Yes, cookies [Clear Cookies and Site Data](#)
 - Have I saved any passwords for this website? No [View Saved Passwords](#)
- Technical Details**
 - Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
 - The page you are viewing was encrypted before being transmitted over the Internet.
 - Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

A red arrow points to the 'View Certificate' button in the 'Security' tab.

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

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...

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



De underliggende problemene....



= 1 av 2 matematiske problemer

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

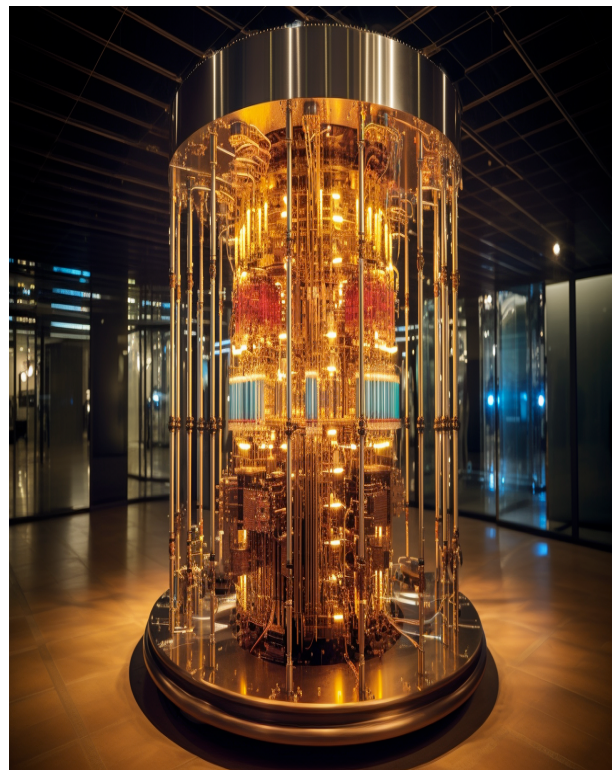


De underliggende problemene....



= 1 av 2 matematiske problemer

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



Kvantemaskiner???



Bits: 011101000101010000010111...

Kvantemaskiner???



Bits: 011101000101010000010111...



Qubits: 

Kan kvantemaskiner bli realitet?

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.

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



Kan kvantemaskiner bli realitet?

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.

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



Kan kvantemaskiner bli realitet?

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.

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



Kan kvantemaskiner bli realitet?

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.

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**



NTNU

Kunnskap for en bedre verden

Kvantesikker Kryptografi

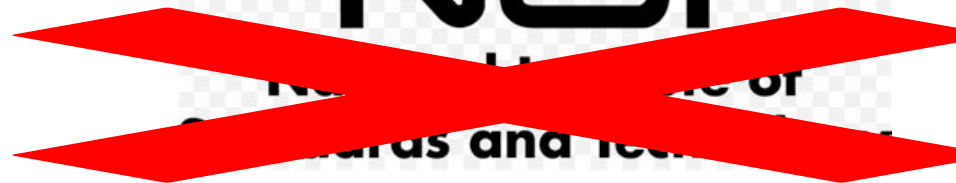


= nye matematiske problemer

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

Nye standarder på vei!

NIST



Not an International **STandard**



NTNU

Kunnskap for en bedre verden

Kvantesikker Kryptografi

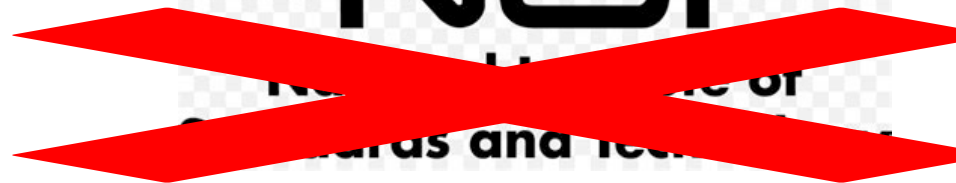


= nye matematiske problemer

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

Nye standarder på vei!

NIST



Not an International **ST**andard



NSM



NTNU

Kunnskap for en bedre verden

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



FakelACR @FakeIACR · Jun 20



2



13



72



5,335

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?

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.

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



Hva om kvantemaskiner aldri kommer?

QUANTUM COMPUTING

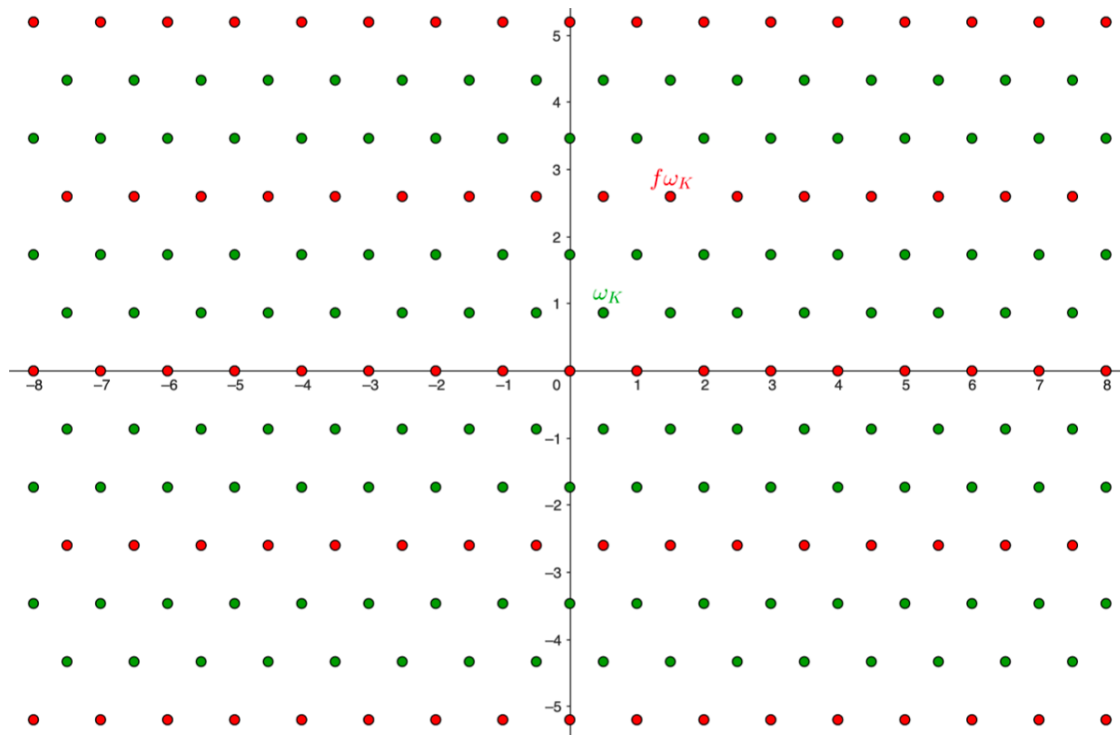
New Algorithm Closes Quantum Supremacy Window

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.

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