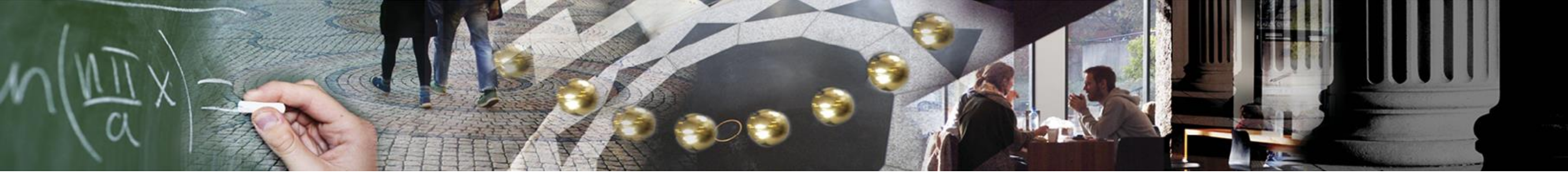


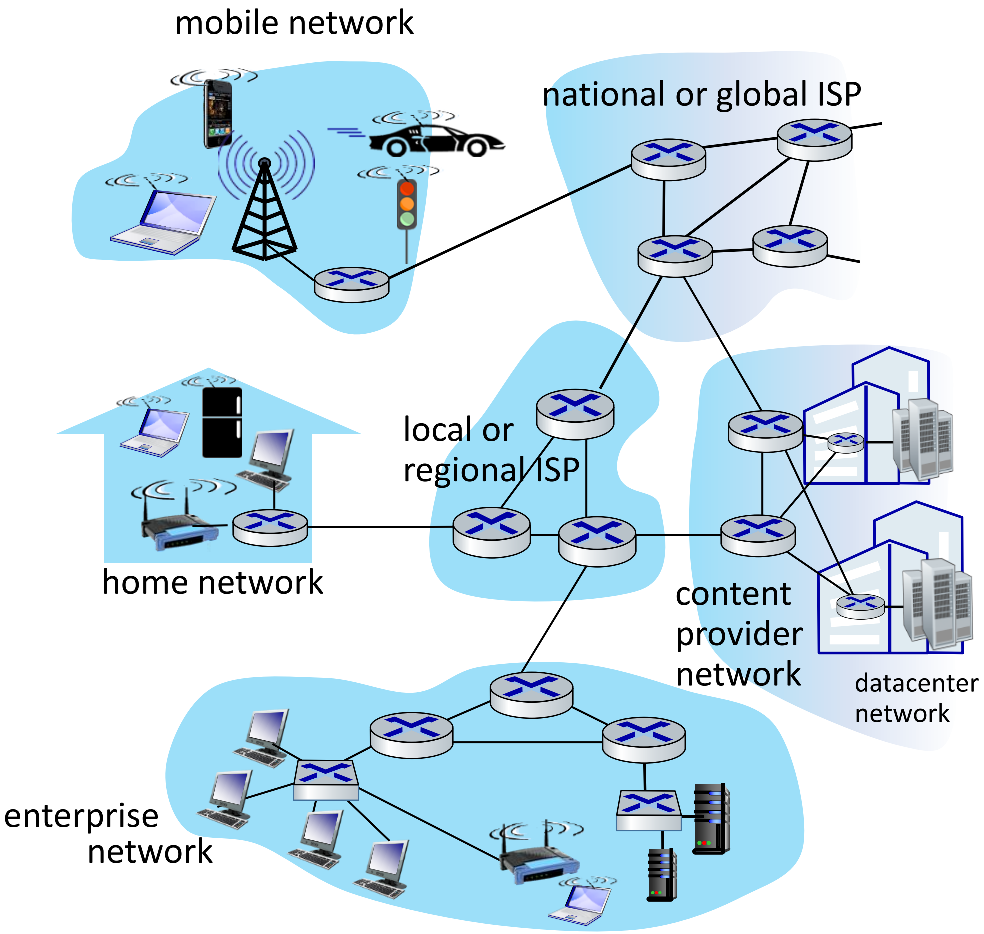
UiO : University of Oslo

Information technology in the health sector (DIGHEL4360)

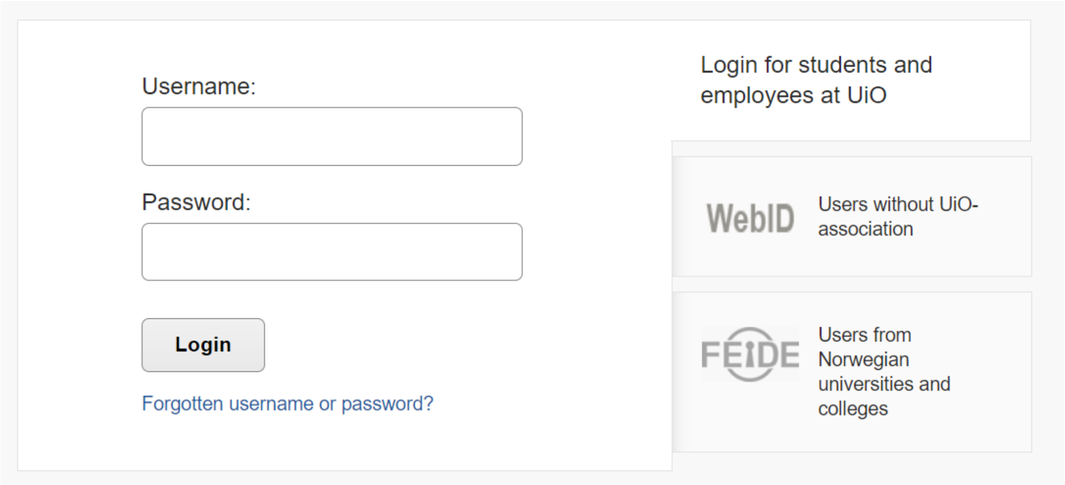
Security II – Security for the World Wide Web

Recapitulation: The Internet

- All communication (e.g., surfing on the Web) goes through different networks
- Some providers might have malicious intents
- Government agencies collect data at large network nodes



Confidential Data



Username:

Password:

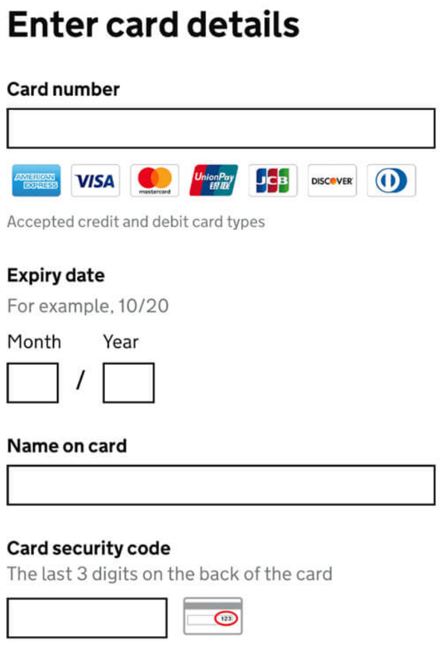
Login

Forgotten username or password?

Login for students and employees at UiO

WebID Users without UiO-association

FEIDE Users from Norwegian universities and colleges



Enter card details

Card number

Accepted credit and debit card types

Expiry date

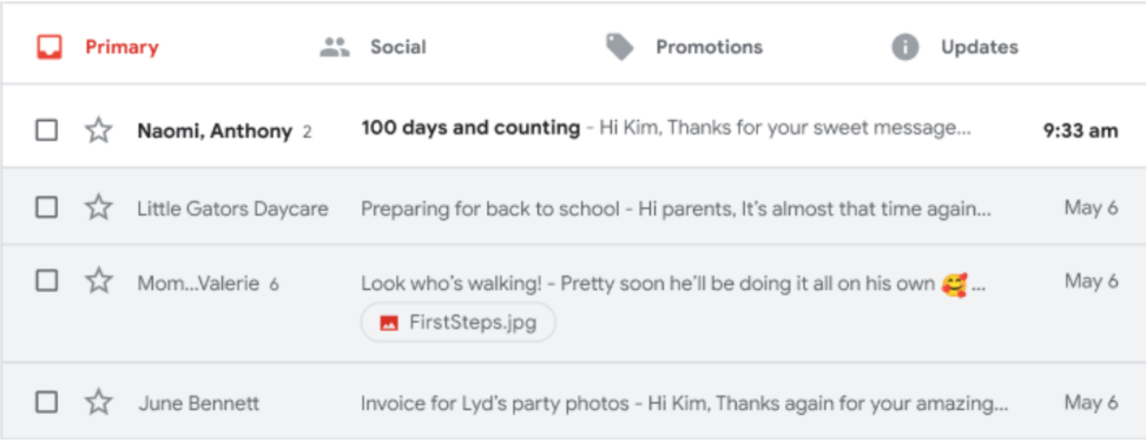
For example, 10/20

Month / Year

Name on card

Card security code

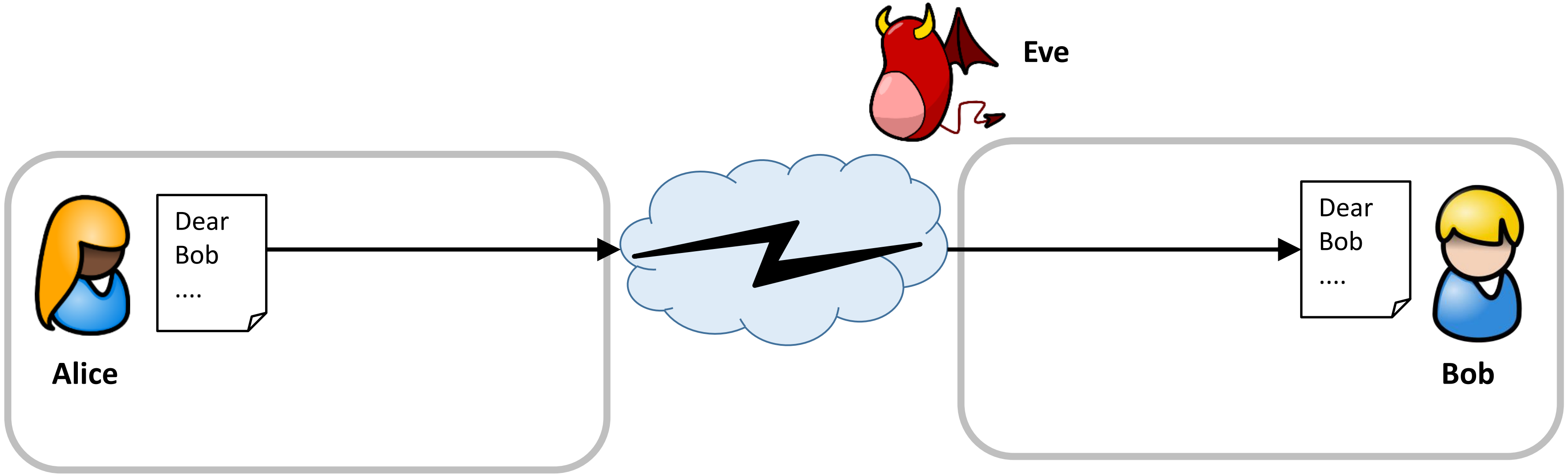
The last 3 digits on the back of the card



Primary Social Promotions Updates

□ ☆	**Naomi, Anthony** 2	**100 days and counting** - Hi Kim, Thanks for your sweet message...	**9:33 am**
□ ☆	Little Gators Daycare	Preparing for back to school - Hi parents, It's almost that time again...	May 6
□ ☆	Mom...Valerie 6	Look who's walking! - Pretty soon he'll be doing it all on his own 🥰 ... FirstSteps.jpg	May 6
□ ☆	June Bennett	Invoice for Lyd's party photos - Hi Kim, Thanks again for your amazing...	May 6

Confidential Communication



Confidential Communication

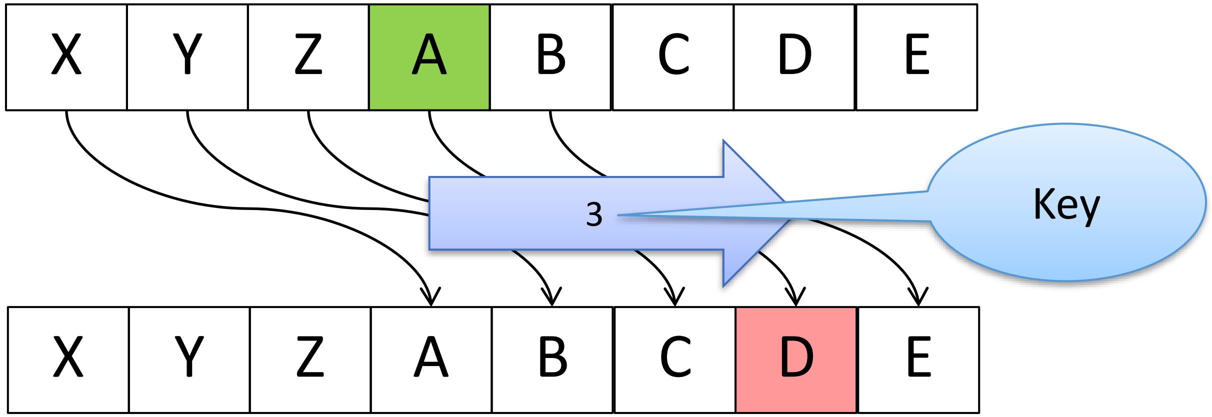
A

B

Image Source: www.asterix.com

Classical Cipher

- Caesar Cipher (50 B.C.)



X	Y	Z	A	B	C	D	E
X	Y	Z	A	B	C	D	E

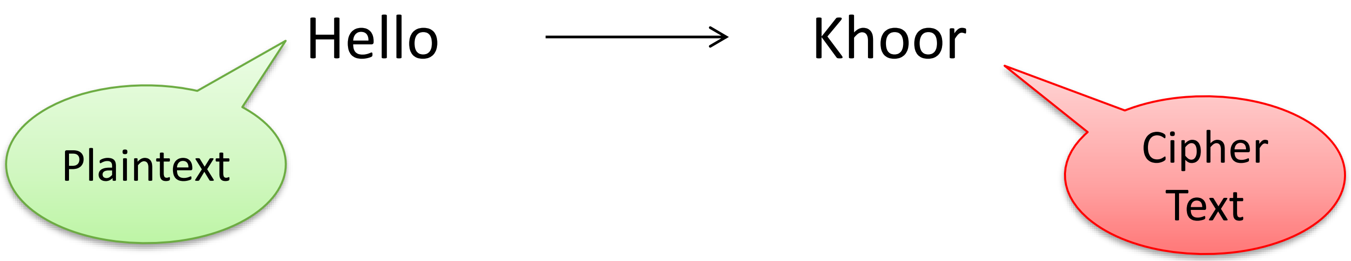


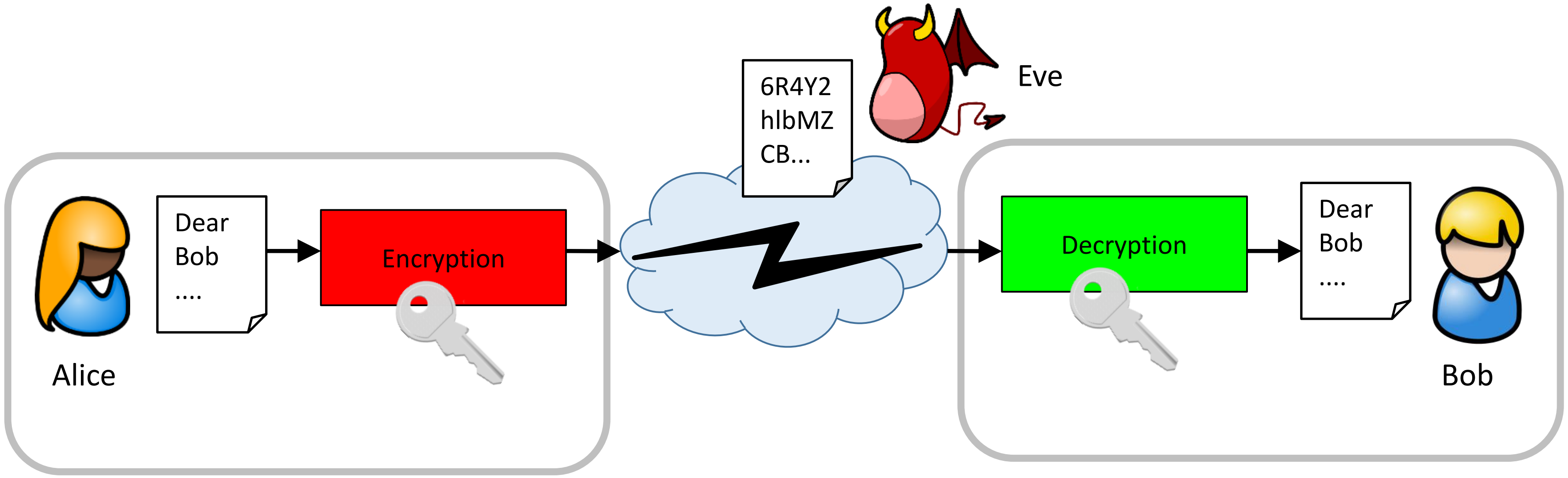
Image Source: www.asterix.com

Encryption

Key = 3

Key = 3

Symmetric Encryption



Caesar Cipher

- Which plaintext is encrypted here?
  - Ymjvznhpgwtbsktcozruxtajwymjqfeditl.
- Try each possible key:
  1. Xliuymgofvsarjsbnyqtwszivxlipedchsk.
  2. Wkhtxlfneurzqiramxpsvryhuwkhodcbgrj.
  3. Vjgswkemdtqyphqzlworuqxgtvjgncbafqi.
  4. Uifrvjdlcspxogpykvnqtpwfsuifmbazeph.
  5. Thequickbrownfoxjumpsoverthelazydog.
  6. Sgdpthbjaqnvmenwitlornudqsgdkzyxcnf.
  7. Rfcosgaizpmuldmvhsknqmtcprfcjyxwbme.
  8. Qebnrfzhyoltkclugrjmplsboqebixwvald.
  9. Pdamqeygxnksjbktfqilokranpdahwvuzkc.
  10. …

Testing all possible values (e.g. of a key) is called **Brute Force Attack**

Enigma

- Invented 1918 by Arthur Scherbius
- Electro-mechanical rotor cipher machines
- Used by the German forces during WWII
- Implements a polyalphabetical substitution cipher
- Number of possible keys: 150,738,274,937,250

Image Source: Wikipedia

Enigma

- Encryption was broken by Polish and British codebreakers in Bletchley Park
- Most famous member:
  - Alan Turing

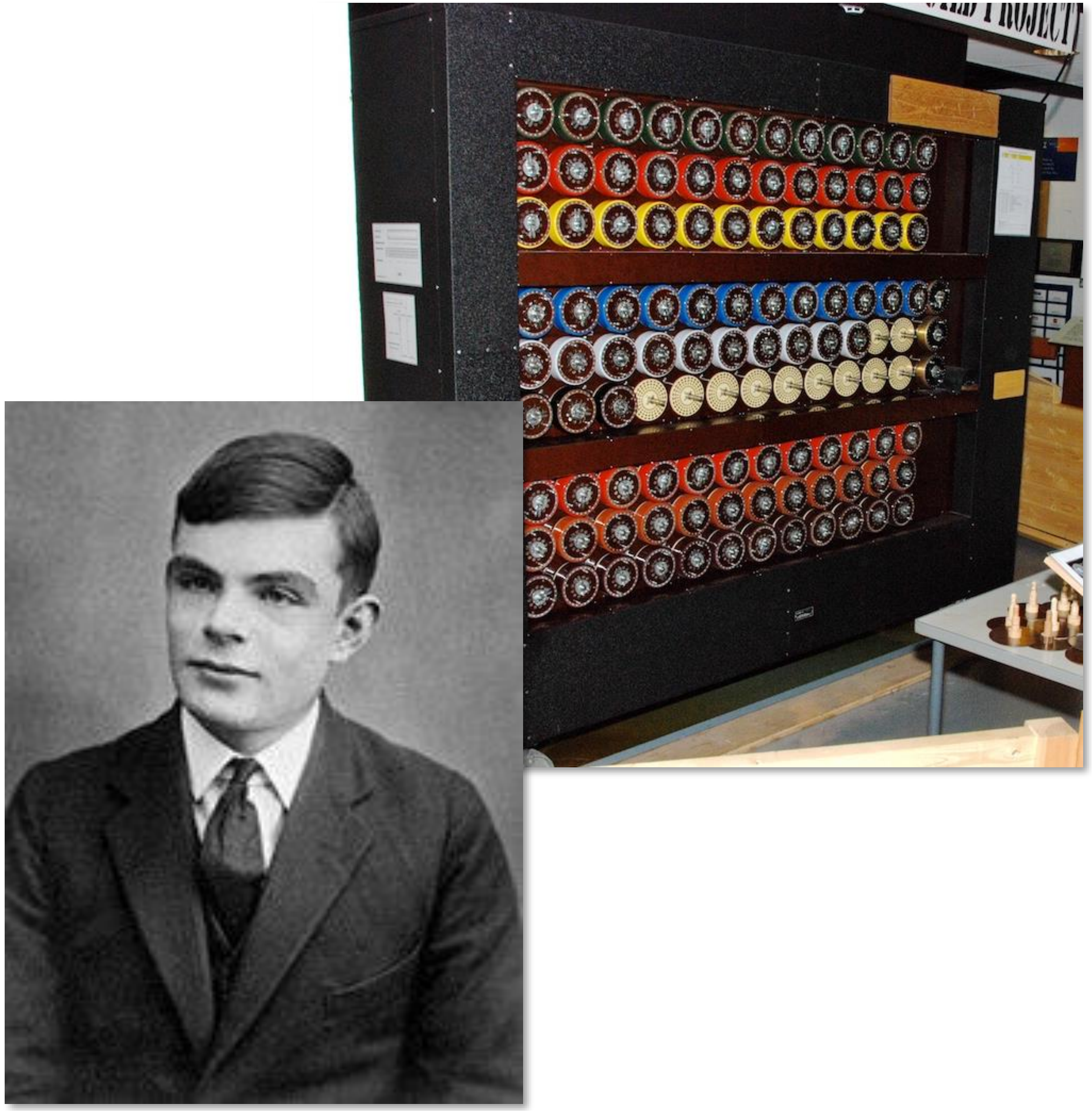
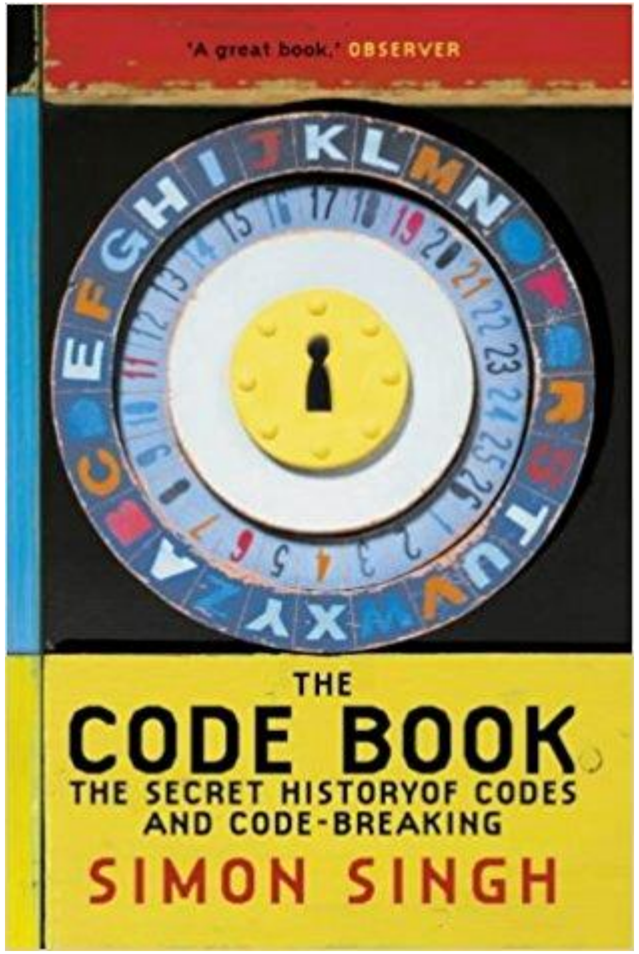


Image Source: http://www.cryptomuseum.com/, Wikipedia

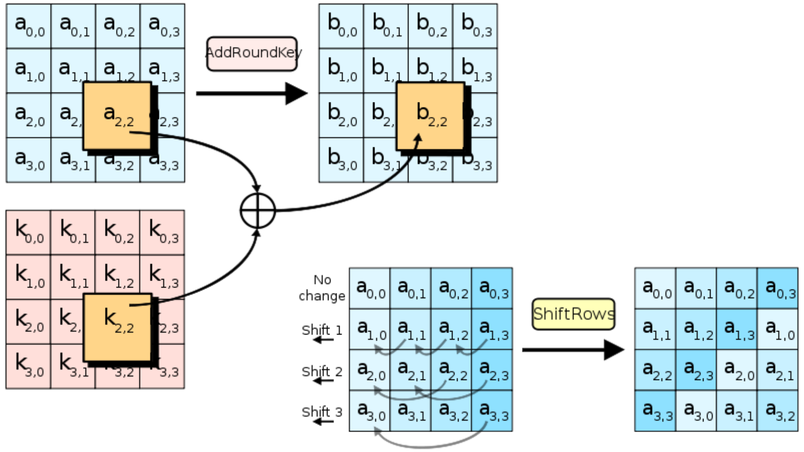
History of Cryptography

- Simon Singh: The Code Book – The Secret History of Codes and Code-breaking

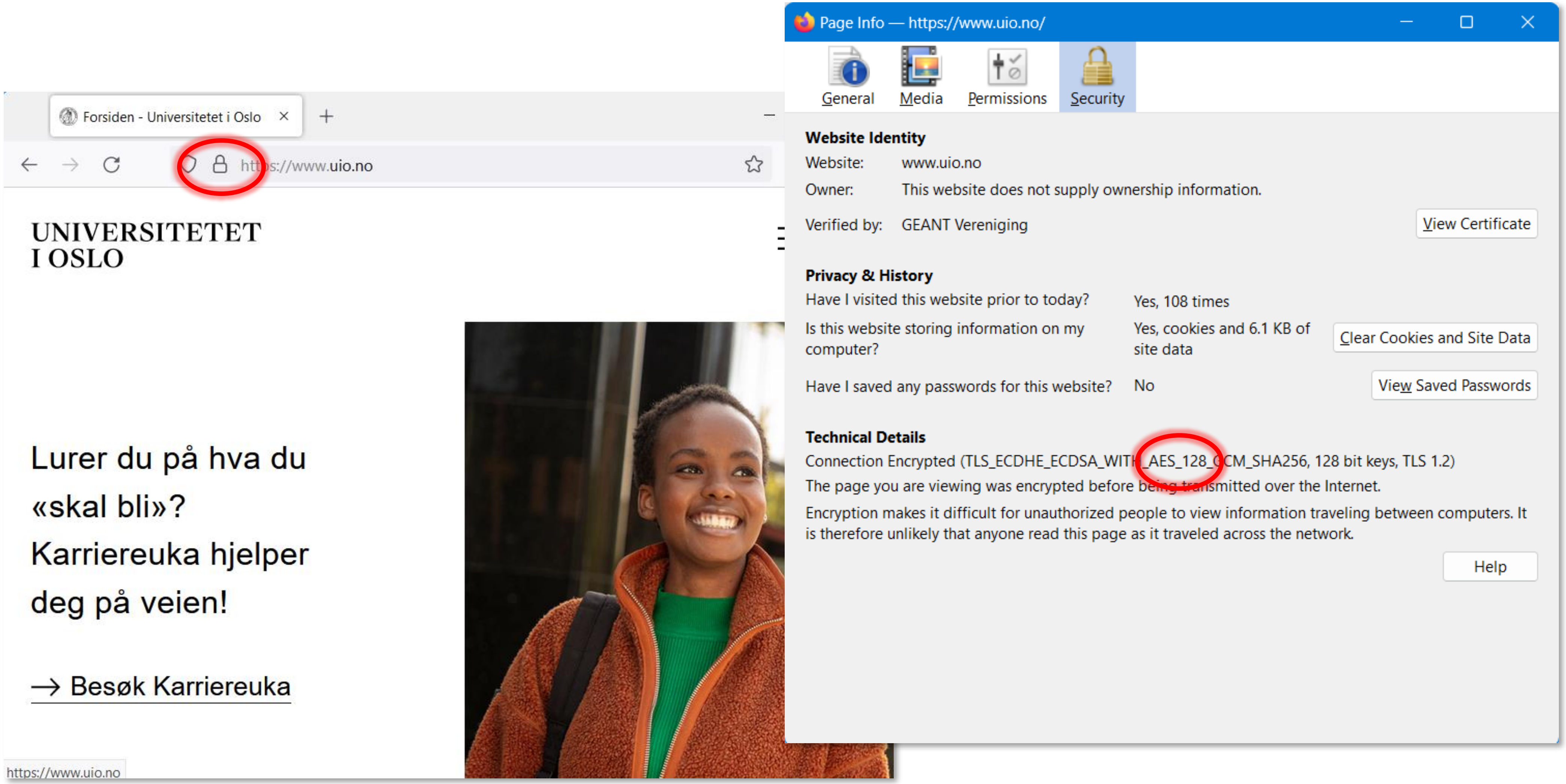


Modern symmetric Encryption

- Advanced Encryption Standard (AES)
  - AES (Rijndael) developed by Belgian cryptographers
  - Standardized by NIST in 2000
  - Keys, plain texts and cipher texts are binary data blocks (not letters)
  - Key length: 128, 192, 256 bit (≈ 32 letters)
- Brute force attack on 128 or 256 bit key? (Assumption: breaking 56 bit in 1 second → in reality more)



Key length	Duration
56 bit	1 s
64 bit	4 m
80 bit	194 d
112 bit	10^9 a
128 bit	10^{14} a
192 bit	10^{33} a
256 bit	10^{52} a



Forsiden - Universitetet i Oslo

https://www.uio.no

UNIVERSITETET
I OSLO

Lurer du på hva du «skal bli»? Karriereuka hjelper deg på veien!

→ Besøk Karriereuka

https://www.uio.no

Page Info — https://www.uio.no/

Website Identity

Website: www.uio.no

Owner: This website does not supply ownership information.

Verified by: GEANT Vereniging

Privacy & History

Have I visited this website prior to today? Yes, 108 times

Is this website storing information on my computer? Yes, cookies and 6.1 KB of site data

Have I saved any passwords for this website? No

Technical Details

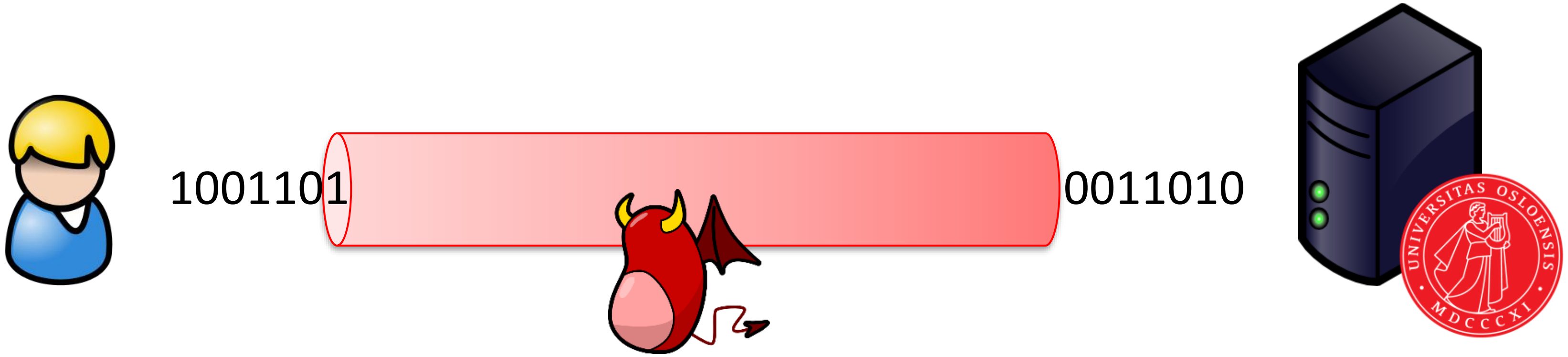
Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

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.

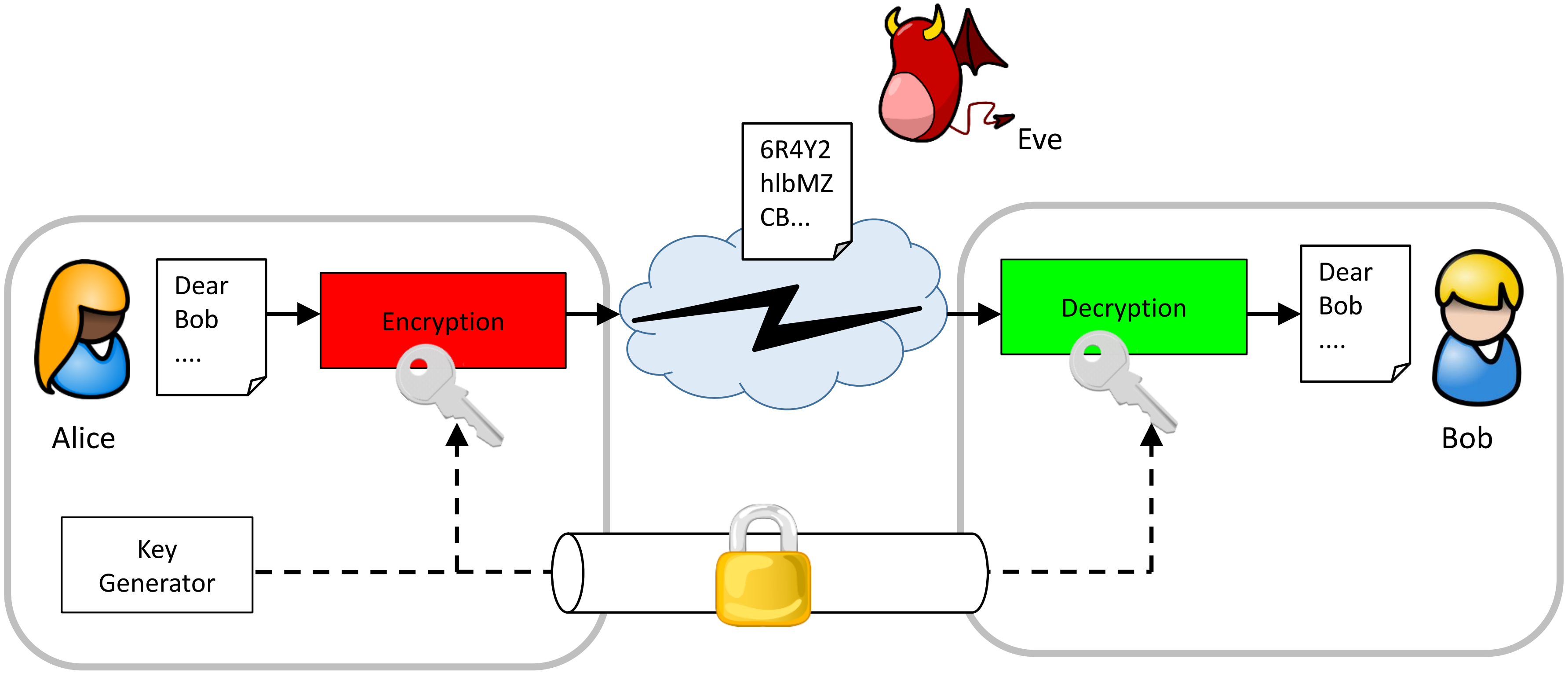
HTTPS / TLS / SSL

- Protects all communication from an adversary eavesdropping on the network.



Symmetric Encryption

- Remaining problem: key exchange



Diffie Hellman Key exchange

- Creating common (symmetric) key only known to the communication partners
- Created by Whitfield Diffie and Martin Hellman in 1976

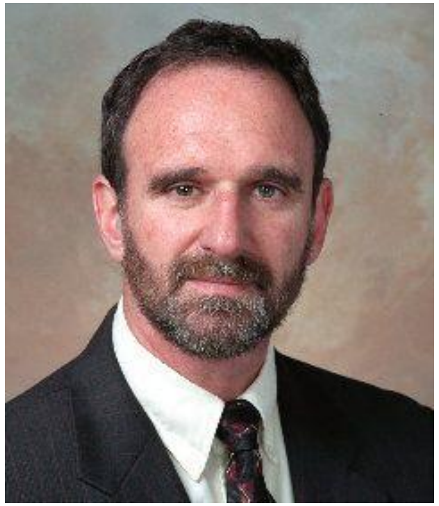


Image source: Wikipedia

Illustration of DH Key Exchange

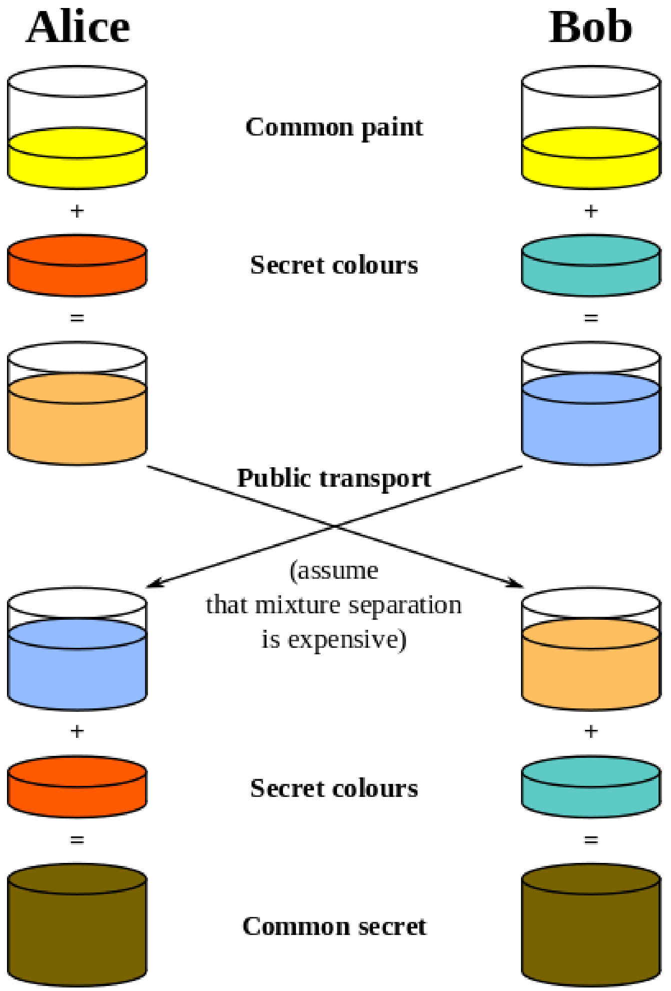
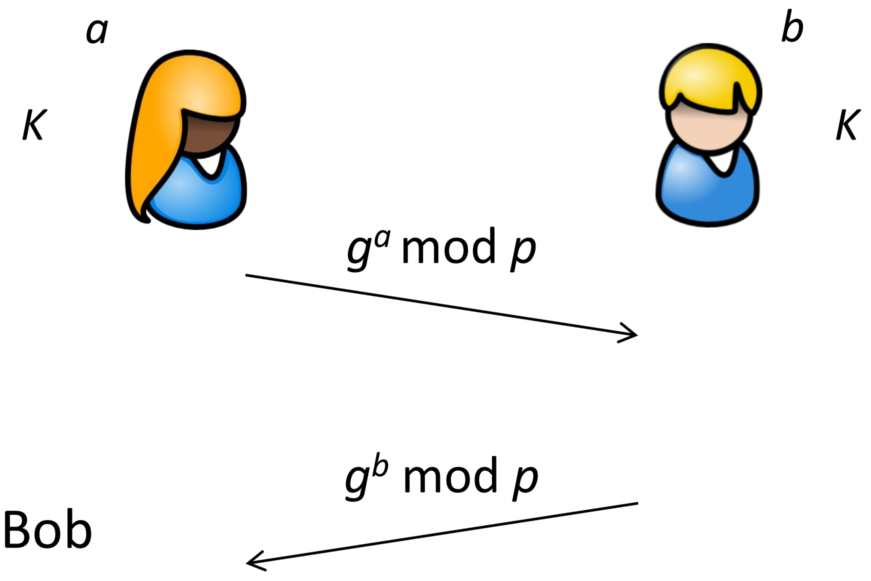


Image source: Wikipedia

Diffie Hellman Key exchange



- Alice and Bob agree on (public parameters):
  - Large prime number p
  - Generator g (i.e., g is primitive root mod p)
- Alice chooses a random number a and sends g^a mod p to Bob
- Bob chooses a random number b and send g^b mod p to Alice
- Calculation of common secret:

  $$\left.\begin{array}{l}\text{– Alice: } (g^b)^a \bmod p \\ \text{– Bob: } (g^a)^b \bmod p\end{array}\right\} = g^{ab} \bmod p = K$$
- Mathematical property of the power/mod function:
  - an attacker can **not** calculate a or b from g^a *or* g^b (discrete logarithm problem)
  - K only known to Alice and Bob

Still a Problem …

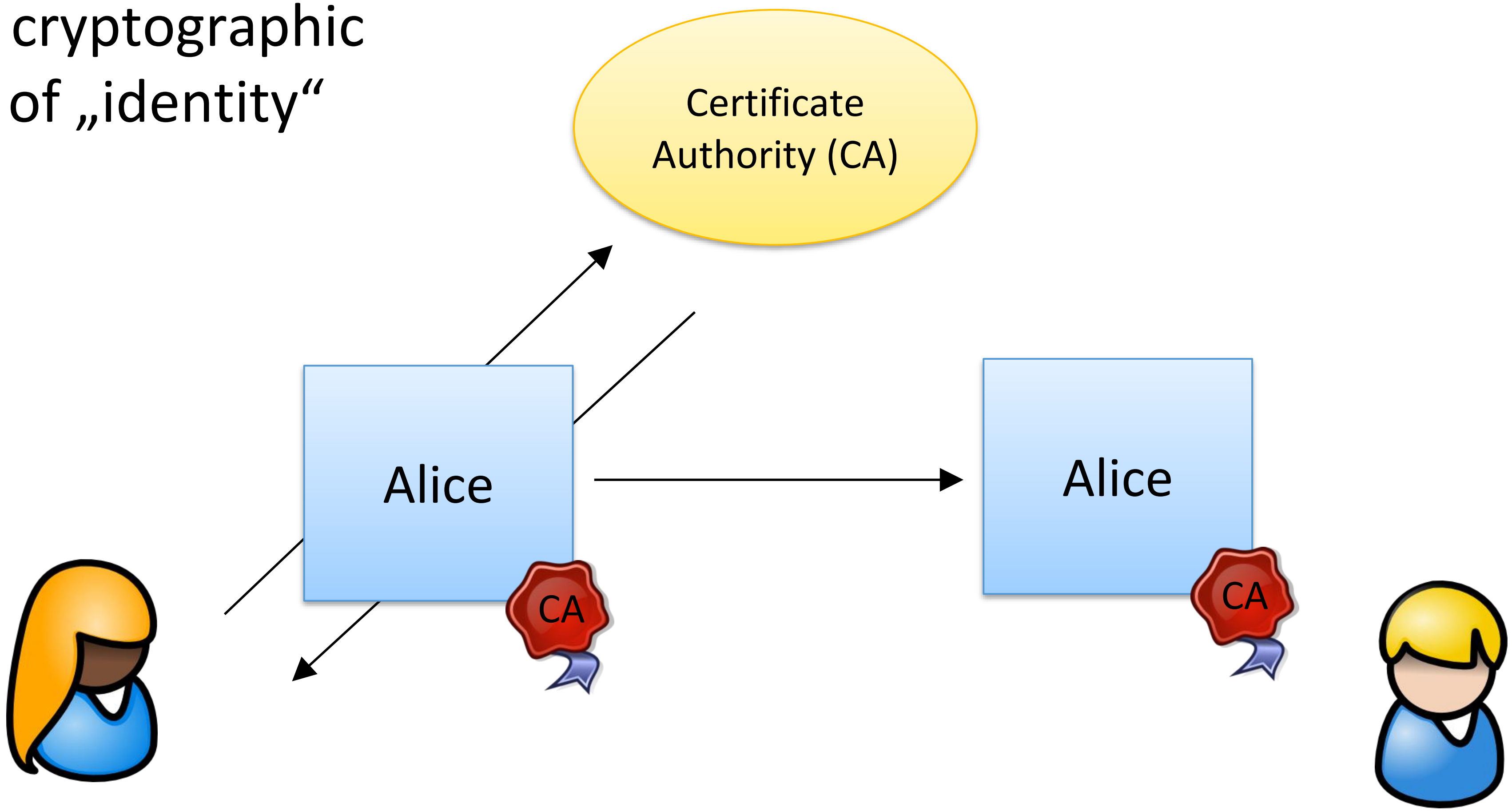
- But how can you be sure who you are talking to?

"On the Internet, nobody knows you're a dog."

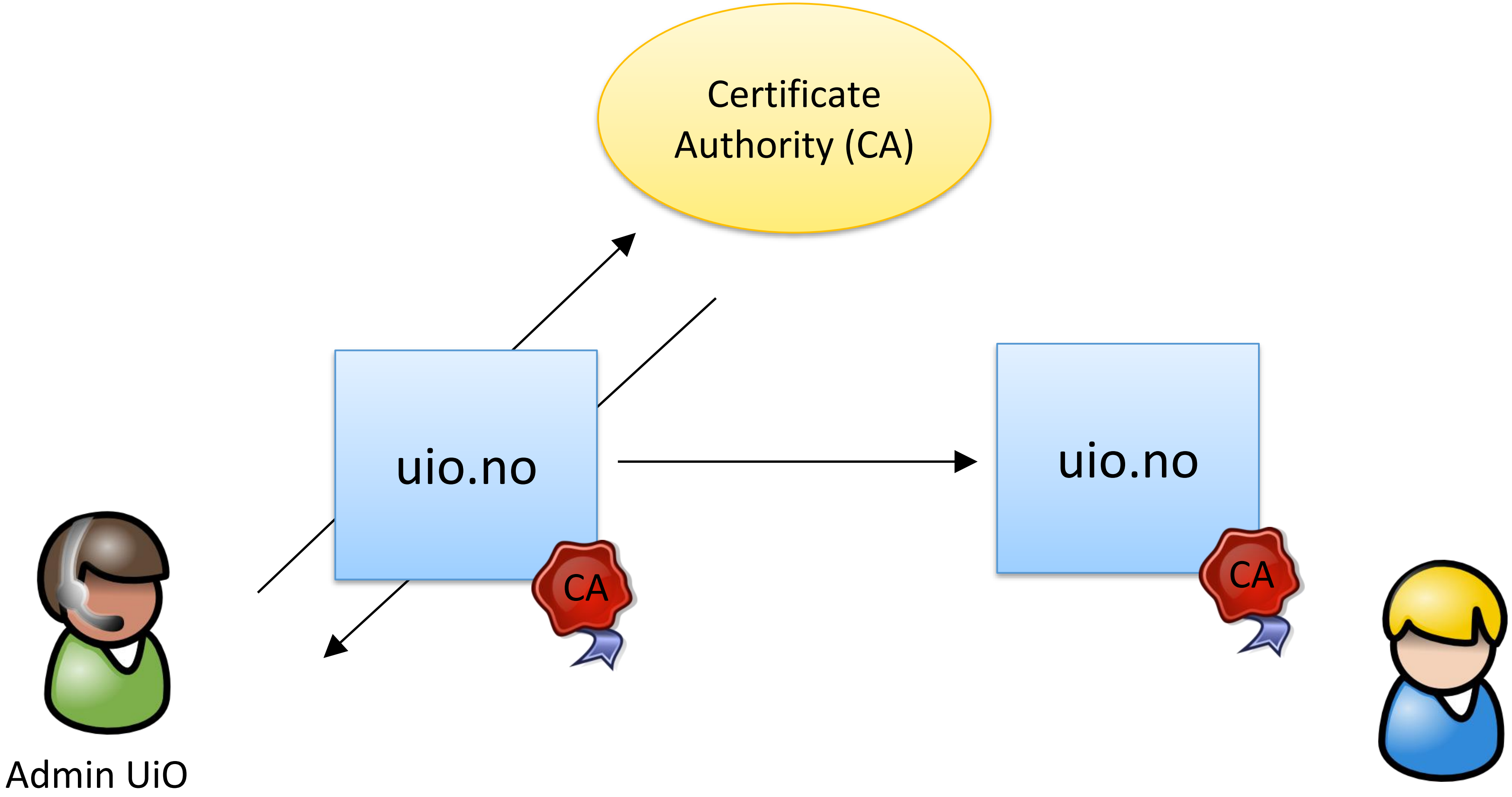
Image Source: The New Yorker cartoon by Peter Steiner, 1993.

Certificates

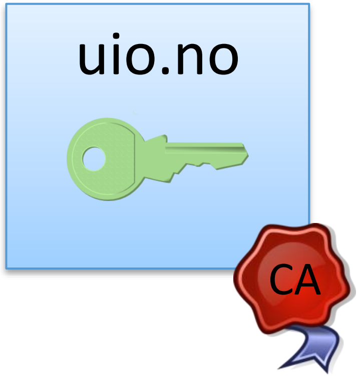
- Allow cryptographic proof of „identity“



Certificates

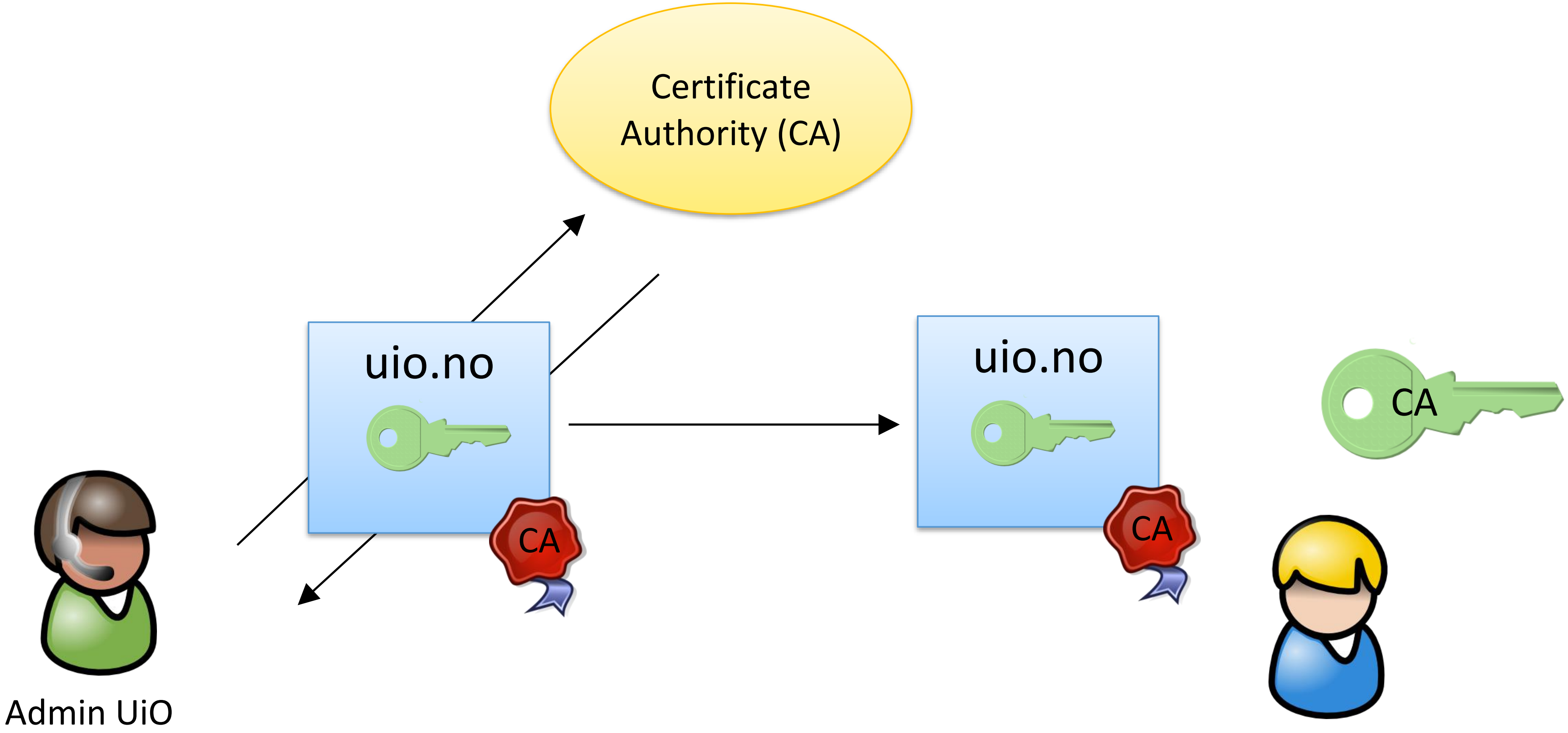


Certificates – more technical

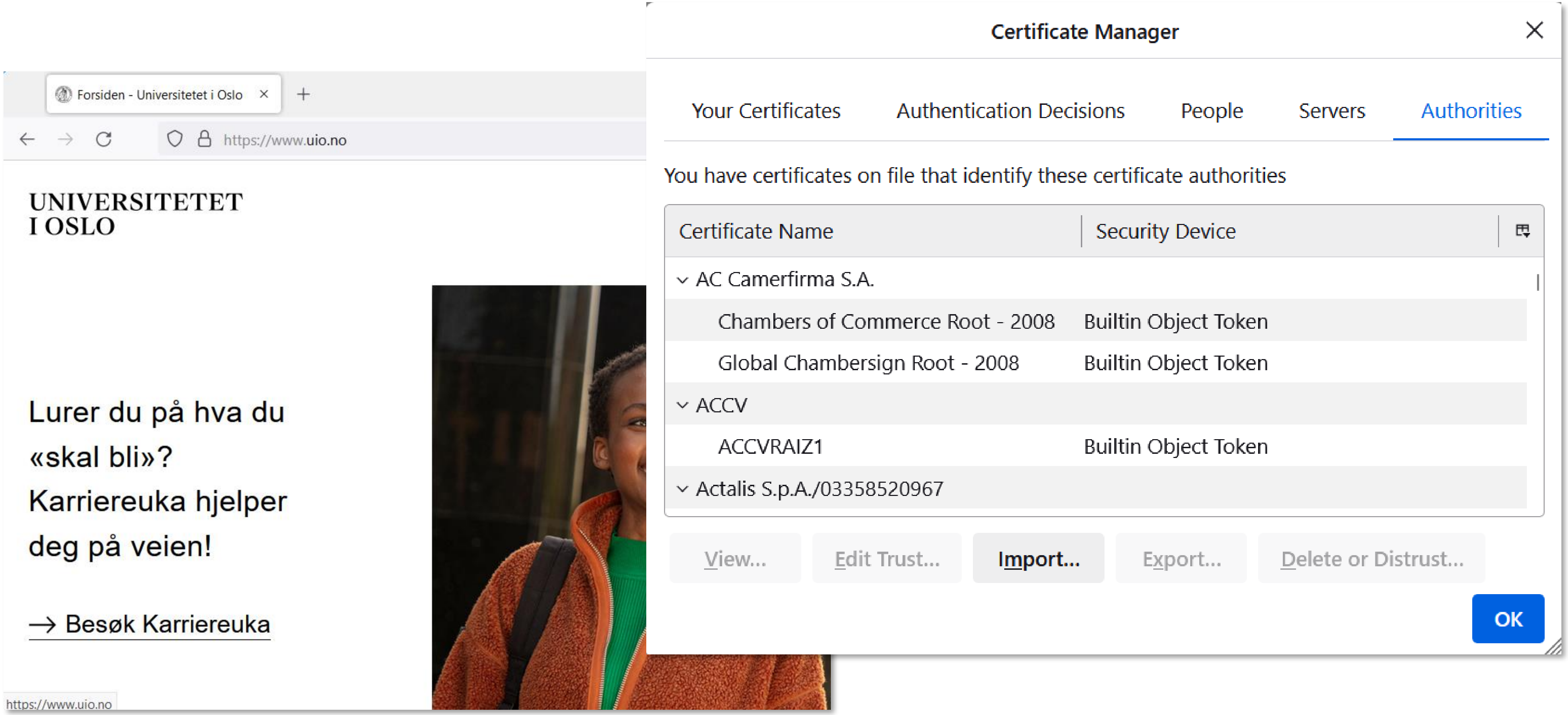


- The certificate contains:
  - An identifier (host name of the Web server)
  - A *cryptographic (public) key*
- The CA creates a *digital signature* that
  - certifies that the CA has verified the identity of the “subject” (here: uio.no)
- The recipient of a digital signature:
  - must *verify* that the signature is *valid*
  - This requires the public key of the issuer

Certificates



Trusted Certificates built-in in the browser



UNIVERSITETET
I OSLO

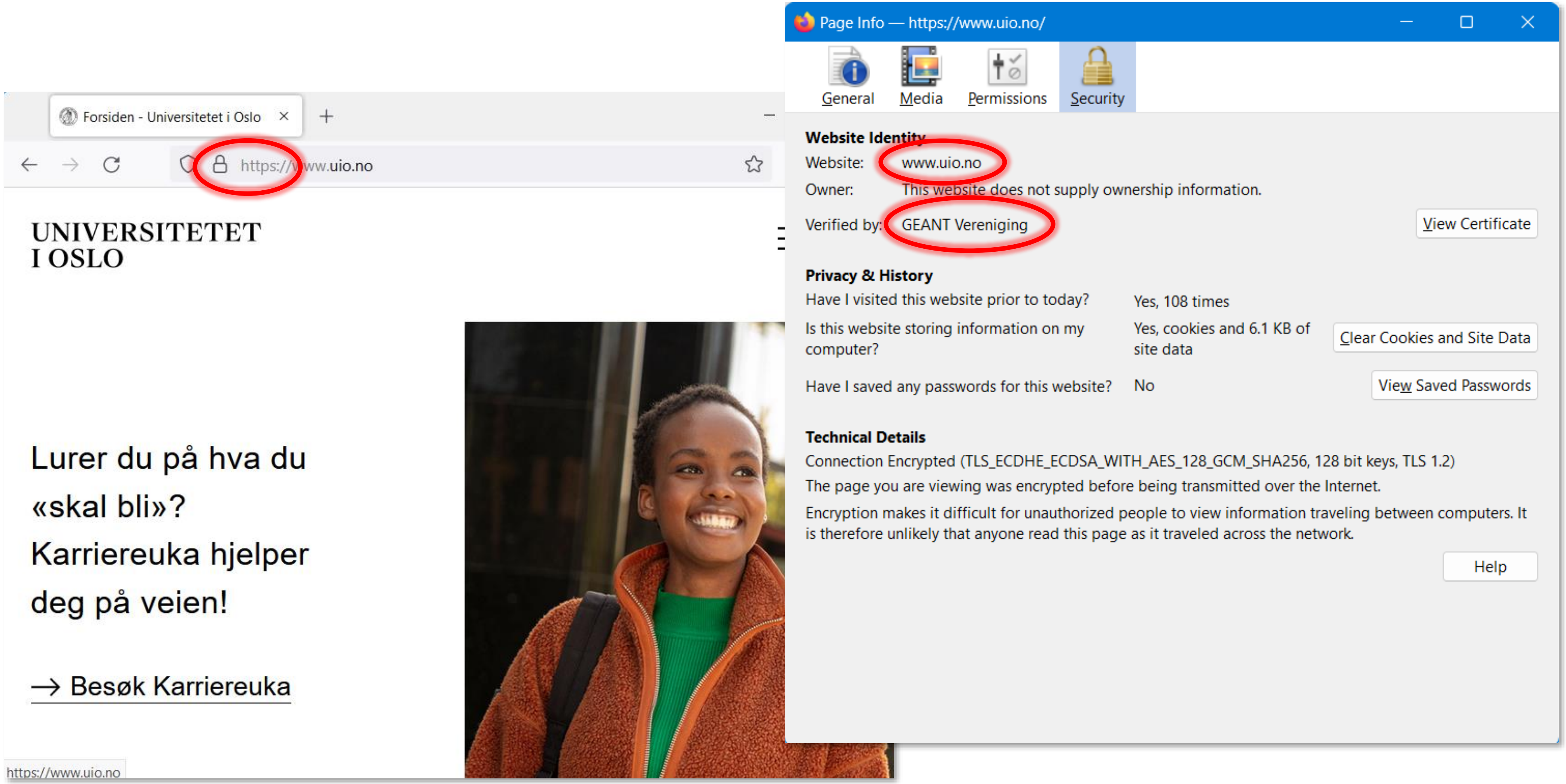
Lurer du på hva du «skal bli»? Karriereuka hjelper deg på veien!

→ Besøk Karriereuka

https://www.uio.no

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	



UNIVERSITETET
I OSLO

Lurer du på hva du «skal bli»? Karriereuka hjelper deg på veien!

→ Besøk Karriereuka

https://www.uio.no

Page Info — https://www.uio.no/

Website Identity

Website: www.uio.no

Owner: This website does not supply ownership information.

Verified by: GEANT Vereniging

Privacy & History

Have I visited this website prior to today?	Yes, 108 times	
Is this website storing information on my computer?	Yes, cookies and 6.1 KB of site data	Clear Cookies and Site Data
Have I saved any passwords for this website?	No	View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

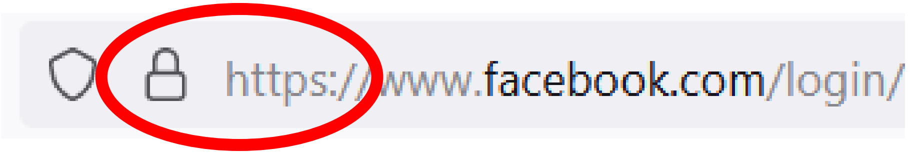
The page you are viewing was encrypted before being transmitted over the Internet.

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.

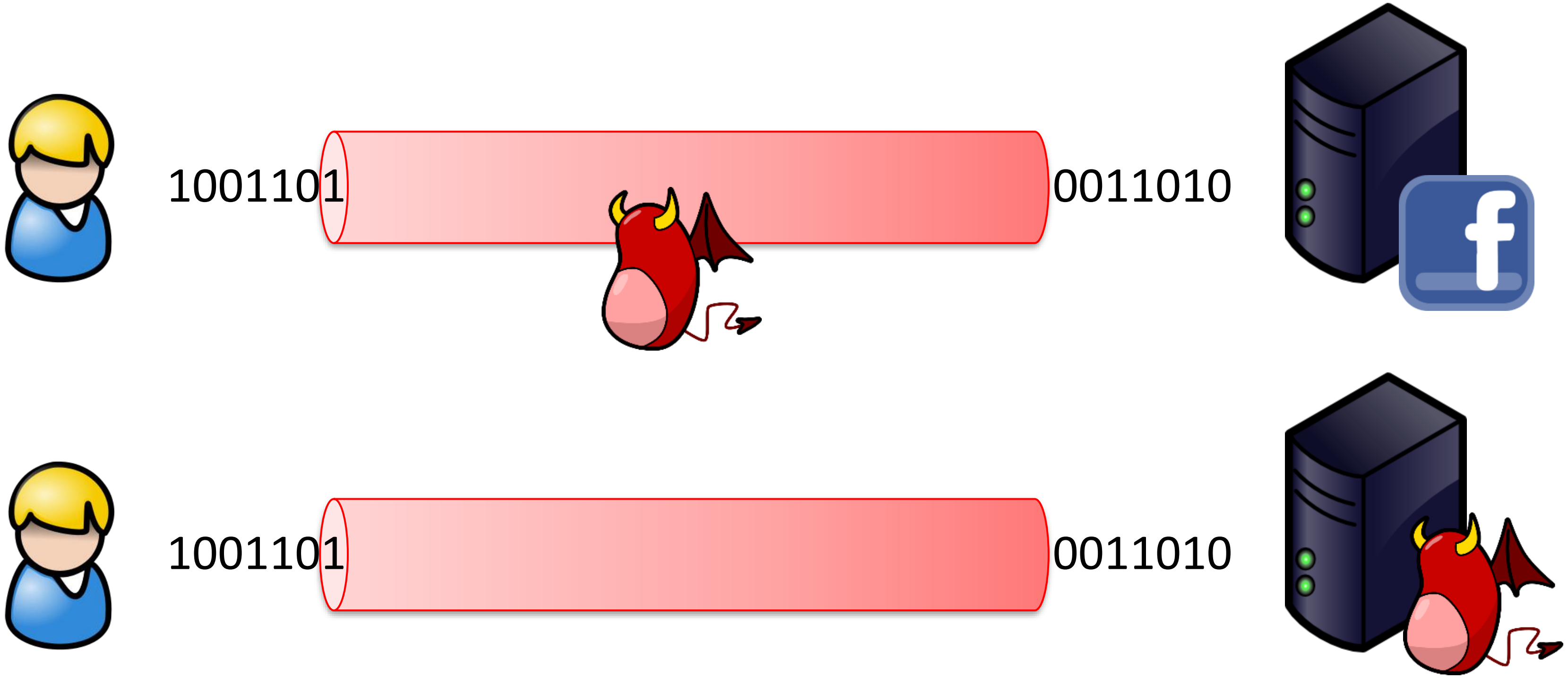
Phishing

- Phishing = „Password Fishing“
  - Victim receives email with link to fake Web site and clicks link
  - Victim enters confidential data (e.g., passwords) assuming it is on a trusted Web site
  - Attacker misuses the entered data
- The tricks …
  - Sending mass emails is very easy and cheap
  - Sender addresses in emails are not authenticated
  - Creating Web sites and mails impersonating a trusted source is easy
  - Hyperlinks to fake Web sites can be hidden in HTML mails

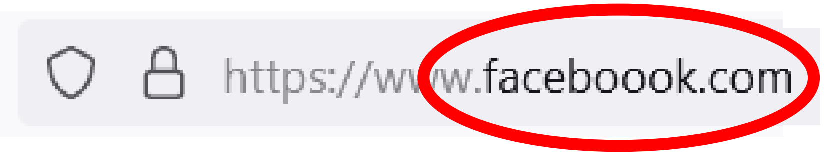
But we used HTTPS …



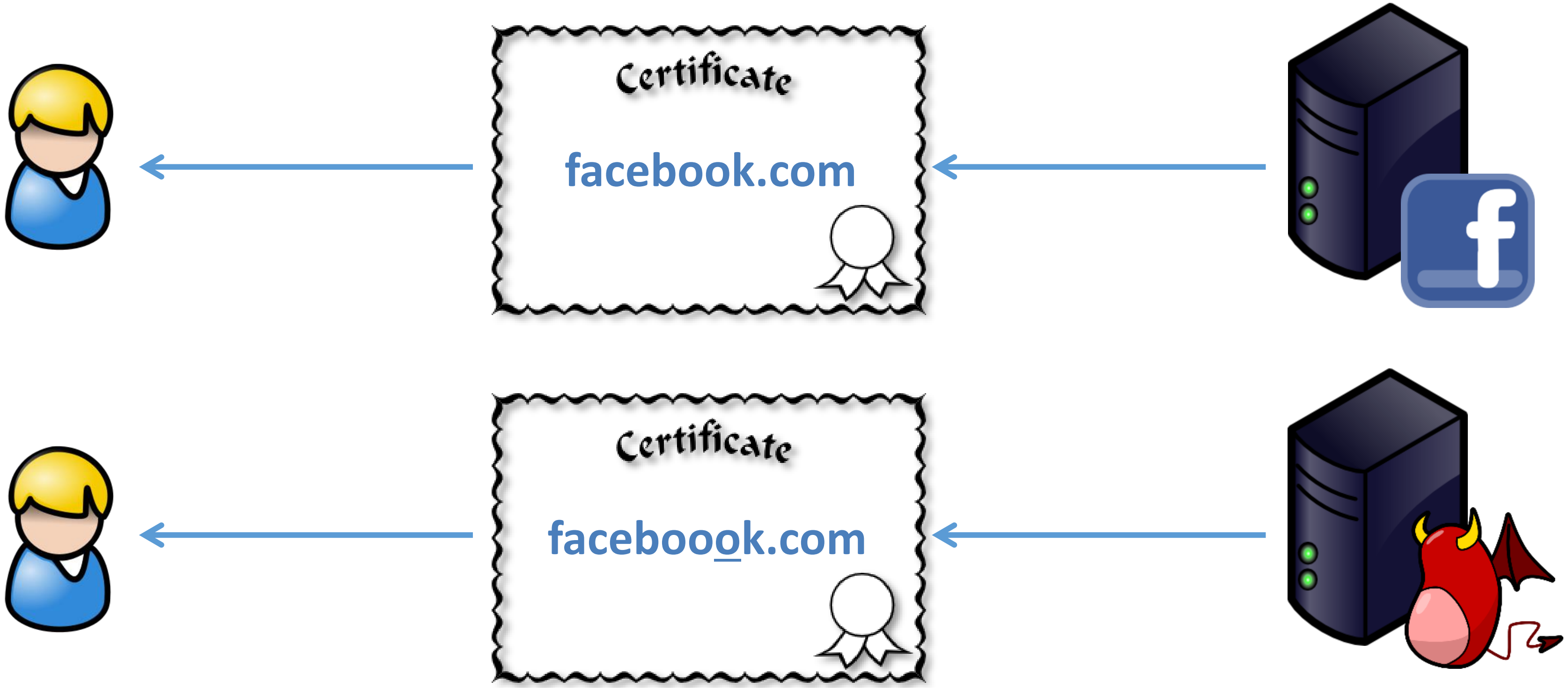
https://www.facebook.com/login/



And the Certificate?

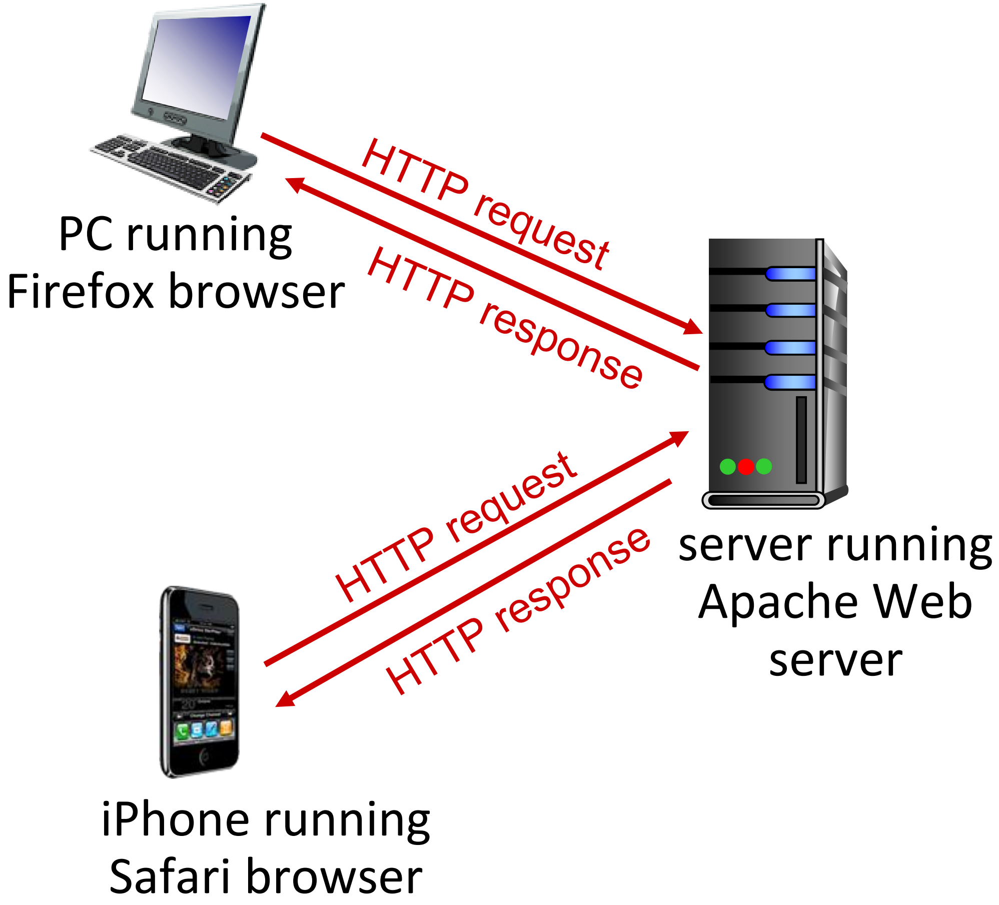


https://www.faceboook.com



HTTP overview

- HTTP: hypertext transfer protocol
- Client/server model:
  - client: browser that requests, receives, (using HTTP protocol) and “displays” Web objects
  - server: Web server sends (using HTTP protocol) objects in response to requests



Source: J.F Kurose and K.W. Ross: Computer Networking

HTTP Request Message

- two types of HTTP messages: request, response
- HTTP request message:
  - ASCII (human-readable format)

carriage return character

line-feed character

request line (GET, POST, HEAD commands)

carriage return, line feed at start of line indicates end of header lines

Source: J.F Kurose and K.W. Ross: Computer Networking

HTTP Response Message

status line (protocol status code status phrase) →

```
HTTP/1.1 200 OK
```

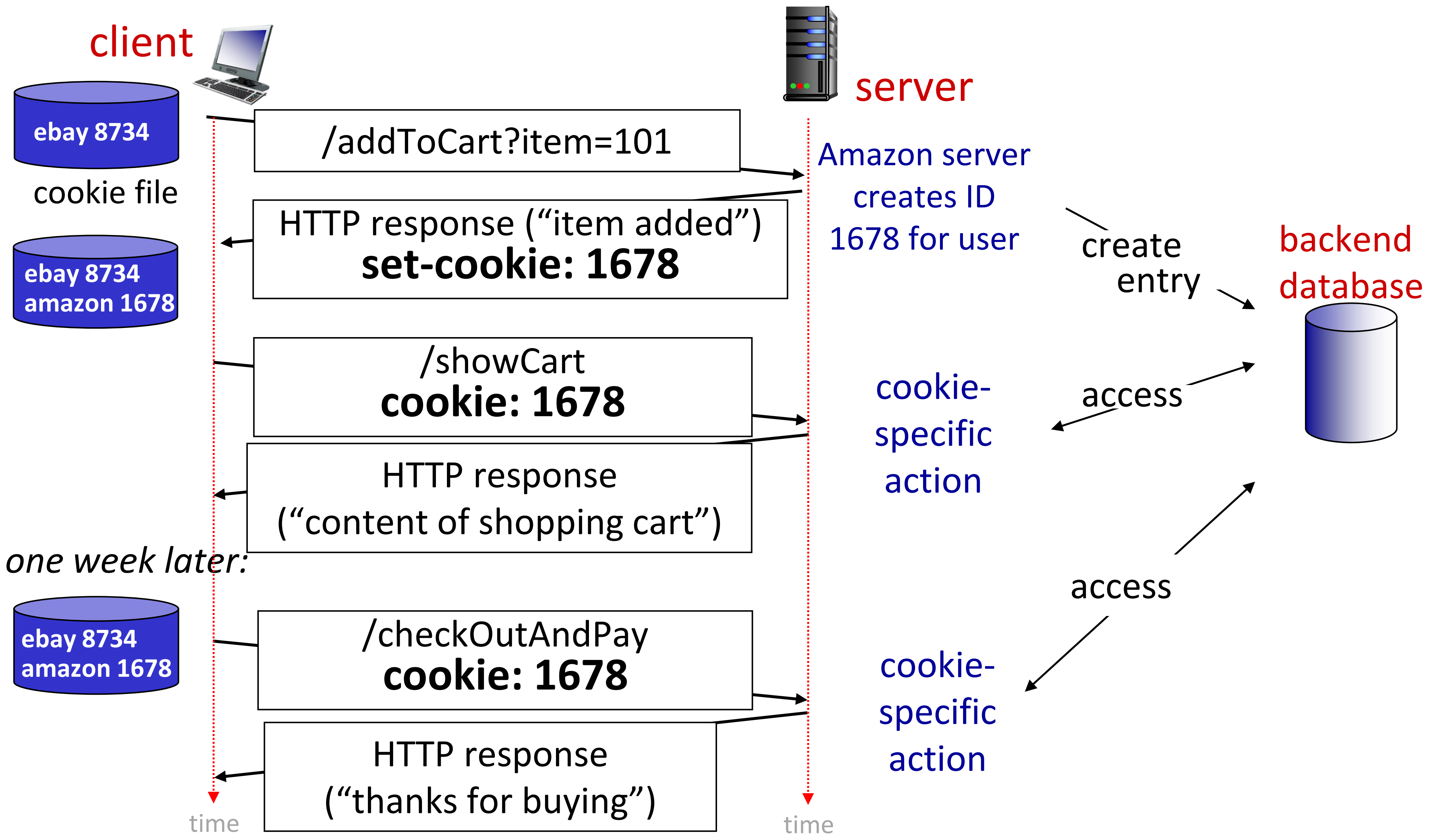
Source: J.F Kurose and K.W. Ross: Computer Networking

Maintaining user/server state: cookies

- HTTP GET/response interaction is stateless
- server maintains no information about past client requests
- no notion of multi-step exchanges of HTTP messages to complete a Web "transaction"
  - no need for client/server to track "state" of multi-step exchange
  - all HTTP requests are independent of each other
  - no need for client/server to "recover" from a partially-completed-but-never-completely-completed transaction
- However …
  - Some applications require a "state", e.g.
    - Shopping: Which items are in the shopping cart?
    - Banking: Is the user already logged in?

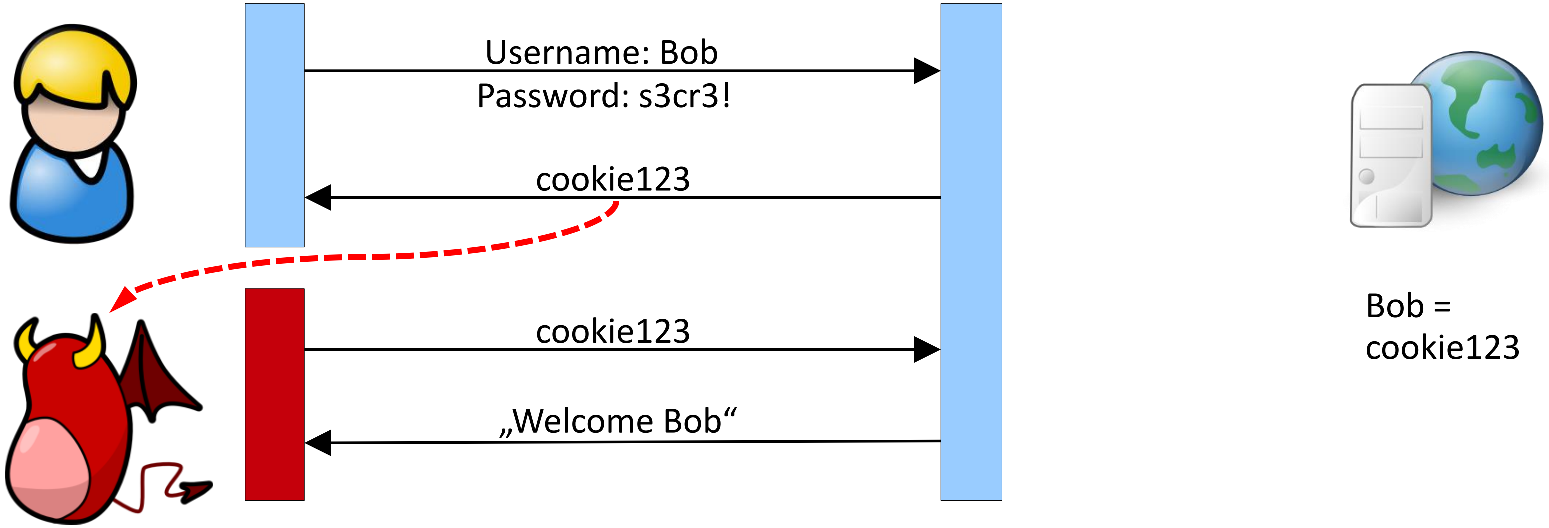
Source: J.F Kurose and K.W. Ross: Computer Networking

Maintaining user/server state: cookies

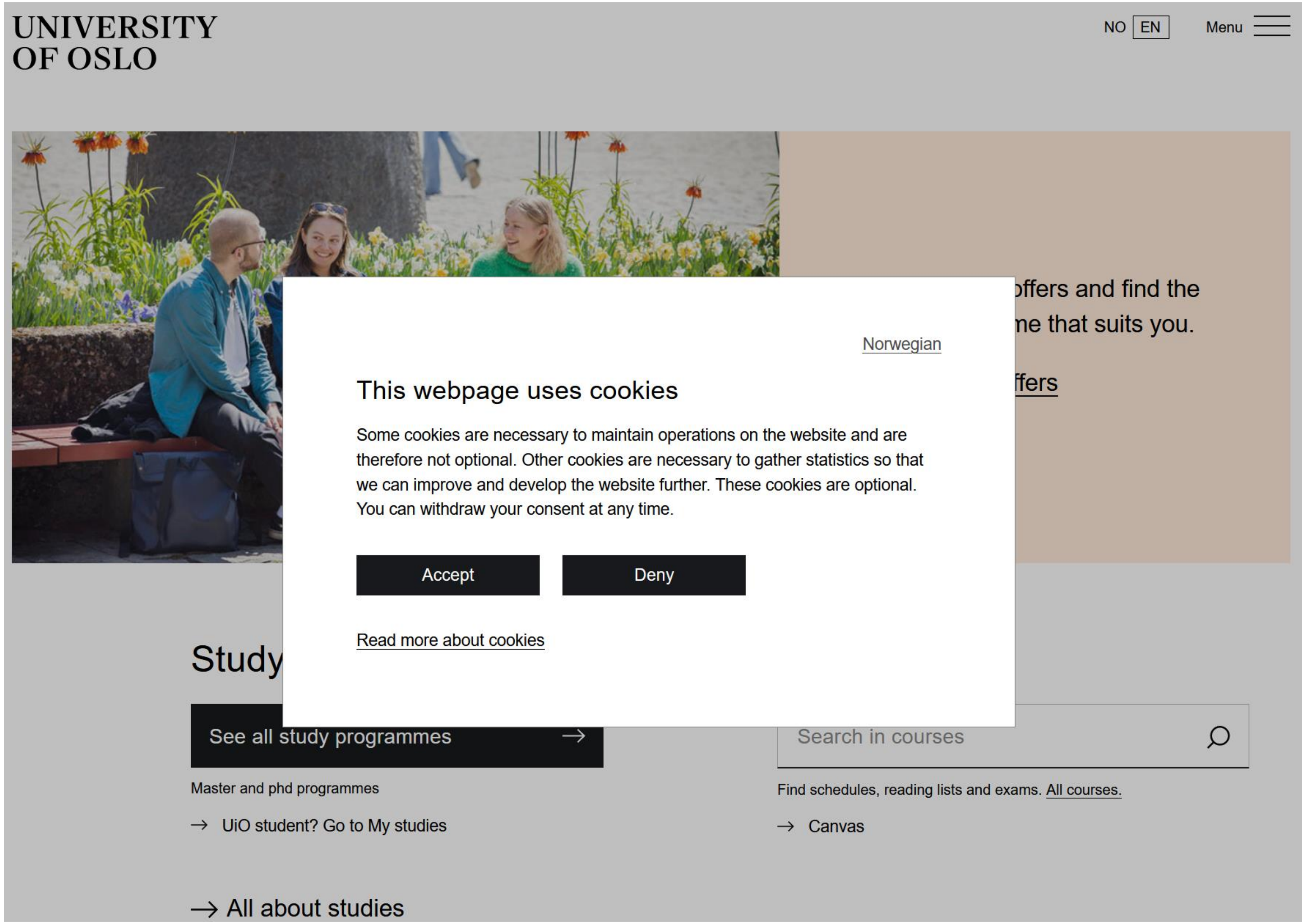


Source: J.F Kurose and K.W. Ross: Computer Networking

Session Stealing



- Cookie Stealing:
  - Network eavesdropping (e.g. inside a WIFI of via ARP Spoofing)
  - Redirecting (e.g. DNS Poisoning)
  - Cross-site scripting



UNIVERSITY
OF OSLO

NO EN Menu

offers and find the
me that suits you.

ffers

Norwegian

This webpage uses cookies

Some cookies are necessary to maintain operations on the website and are therefore not optional. Other cookies are necessary to gather statistics so that we can improve and develop the website further. These cookies are optional. You can withdraw your consent at any time.

Accept Deny

Read more about cookies

Study

See all study programmes →

Master and phd programmes

→ UiO student? Go to My studies

Search in courses

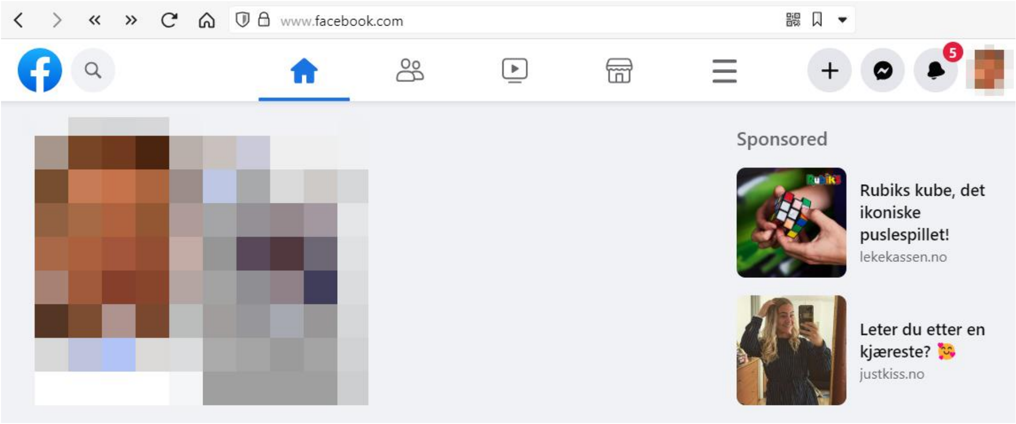
Find schedules, reading lists and exams. All courses.

→ Canvas

→ All about studies

Web Tracking

- Cookies allow to identify users on consecutive “visits” (after 1 min, but also after 1 month)
  - Required for Web shops, banking etc.
  - Enables also tracking of users
- Especially dangerous: “third-party” cookies
  - Used mainly by advertisement networks
  - Can track users over different web pages
  - “Learn” user preferences
  - Show tailored advertisement



Rubiks kube, det ikoniske puslespillet!
lekekassen.no

Leter du etter en kjæreste? 🥰
justkiss.no

Summary

- Encryption is an ancient concept for ensuring data confidentiality
- Key exchange and origin authenticity (who am I talking to) are rather modern methods
- HTTPS ensures confidentiality and authenticity for the Web
- Attention: only ensures that the browser is communicating to the hostname/domain shown in the address bar → check the hostname
- HTTPS does **not** guarantee the trustworthiness of the Web page
- Cookies are an essential part of the Web, but can also be misused for user tracking