



UiO : **University of Oslo**

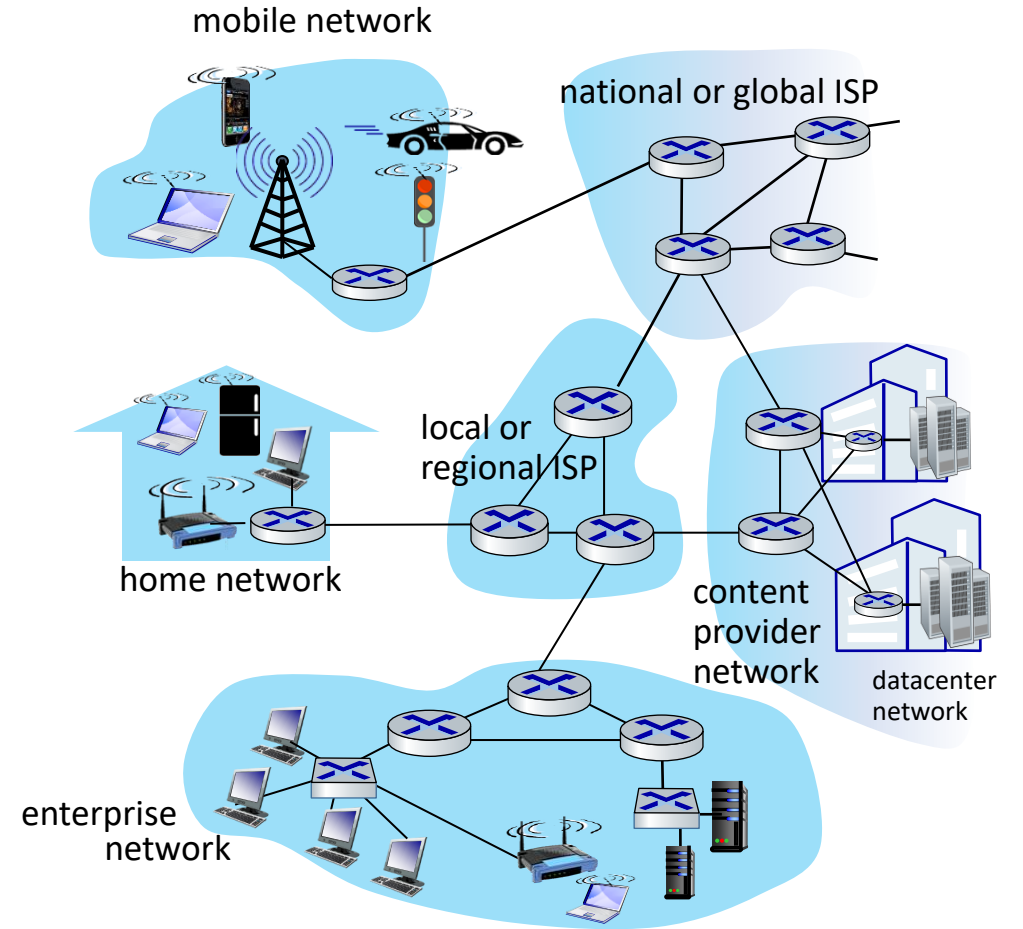
Information technology in the health sector (DIGHEL4360)

Security for the World Wide Web and Email



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:

[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

 /

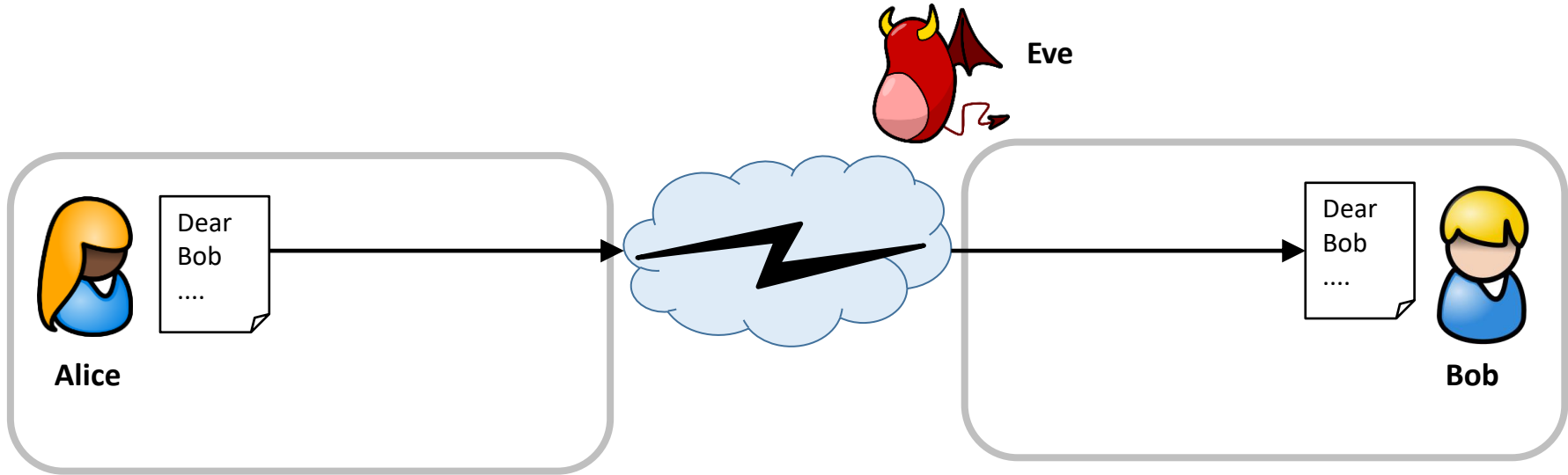
Name on card

Card security code

The last 3 digits on the back of the card

<input type="checkbox"/> Primary	<input type="checkbox"/> Social	<input type="checkbox"/> Promotions	<input type="checkbox"/> Updates
<input type="checkbox"/> ☆ Naomi, Anthony 2	100 days and counting	- Hi Kim, Thanks for your sweet message...	9:33 am
<input type="checkbox"/> ☆ Little Gators Daycare	Preparing for back to school	- Hi parents, It's almost that time again...	May 6
<input type="checkbox"/> ☆ Mom...Valerie 6	Look who's walking!	- Pretty soon he'll be doing it all on his own 🥳 ...	May 6
<input type="checkbox"/> ☆ June Bennett	Invoice for Lyd's party photos	- Hi Kim, Thanks again for your amazing...	May 6

Confidential Communication

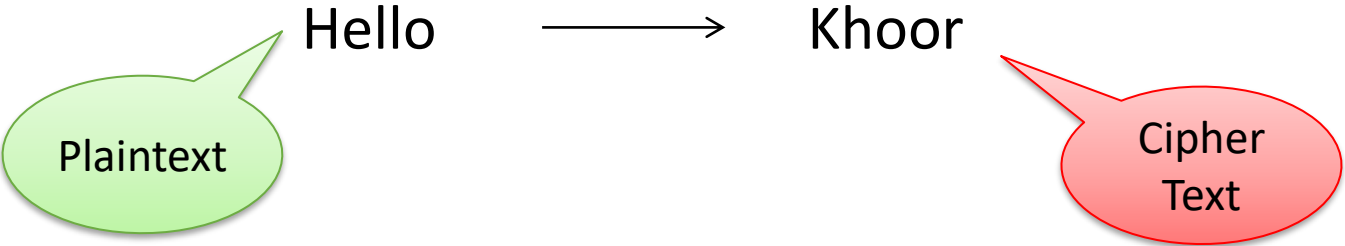
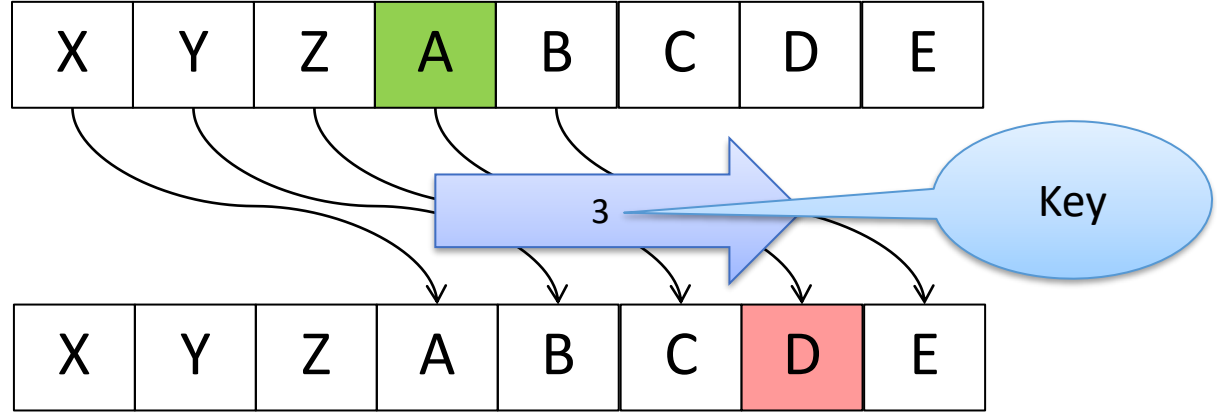


Confidential Communication



Classical Cipher

- Caesar Cipher (50 B.C.)



Encryption

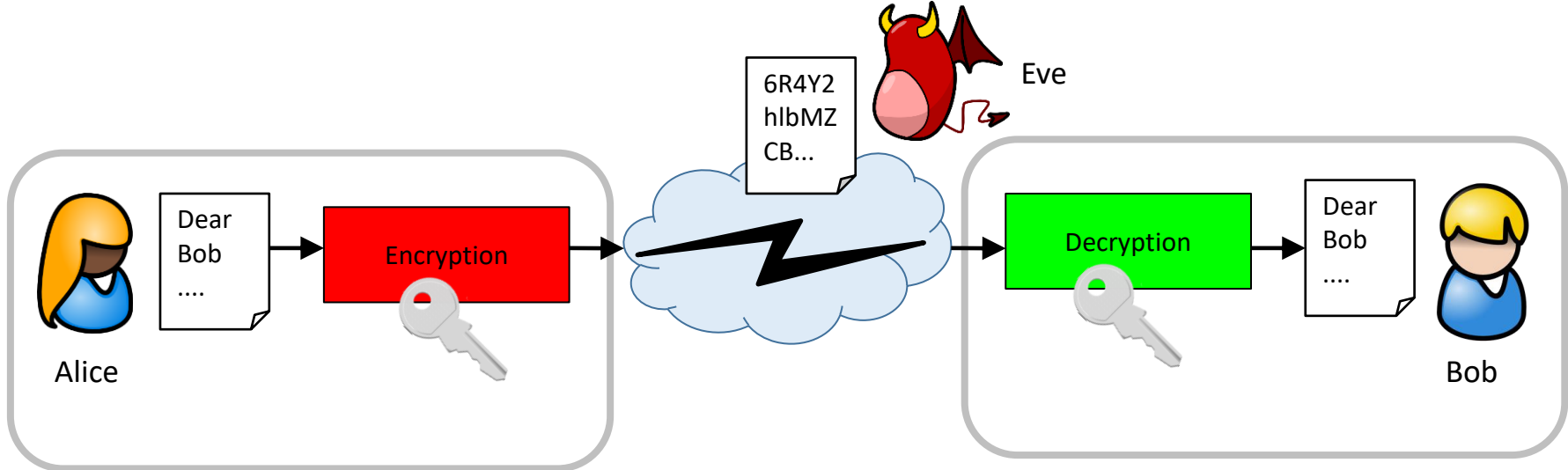
Key = 3



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. Pdamqeygxnskjbktfqilokranpdahwvuzkc.
 10. ...

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

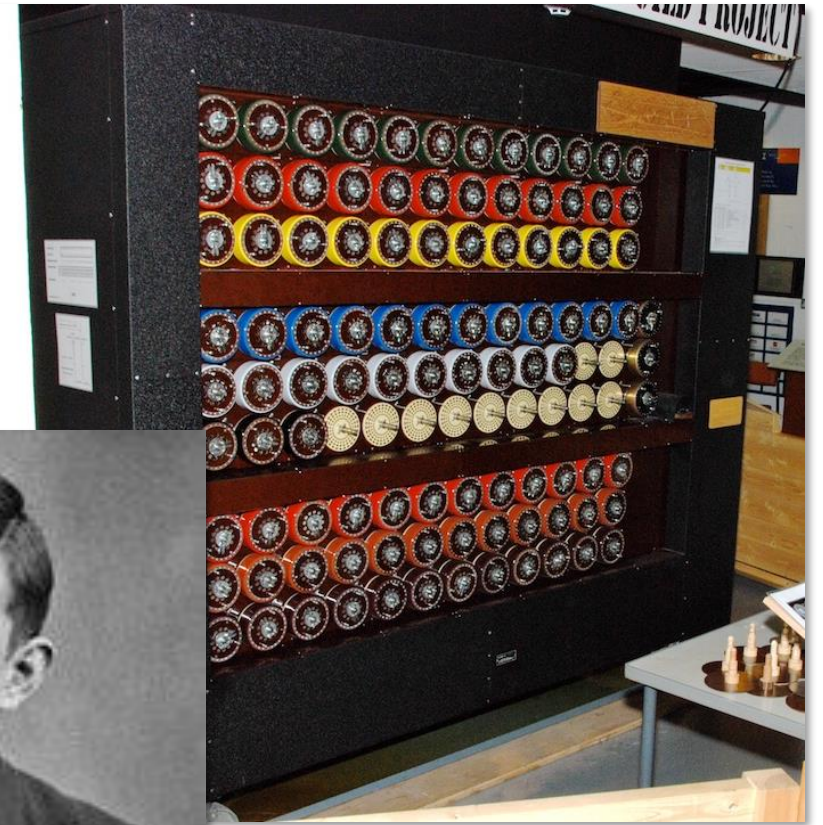
Enigma

- 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



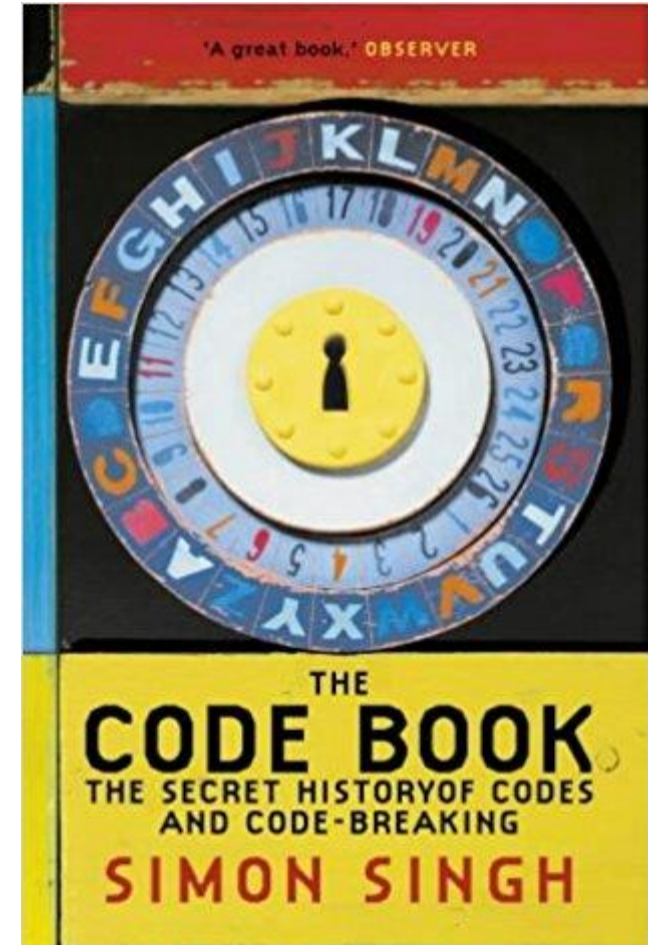
Enigma

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



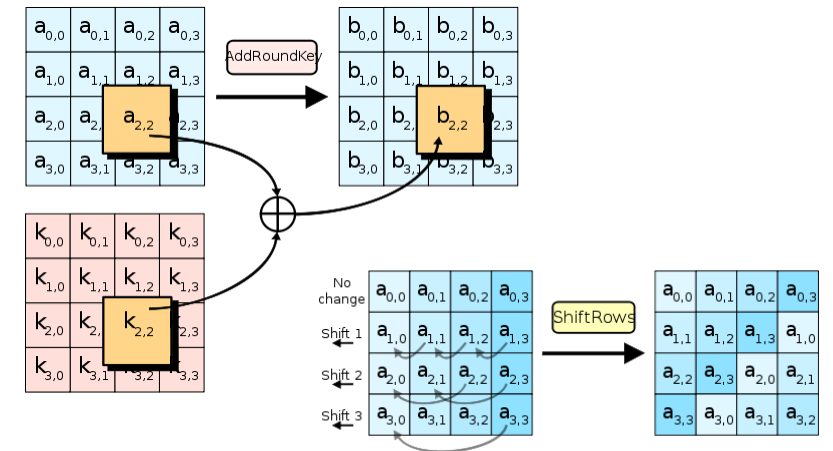
History of Cryptography

- 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 (\approx 32 letters)
- Brute force attack on 128 or 256 bit key? (Assumption: breaking 56 bit in 1 second \rightarrow 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

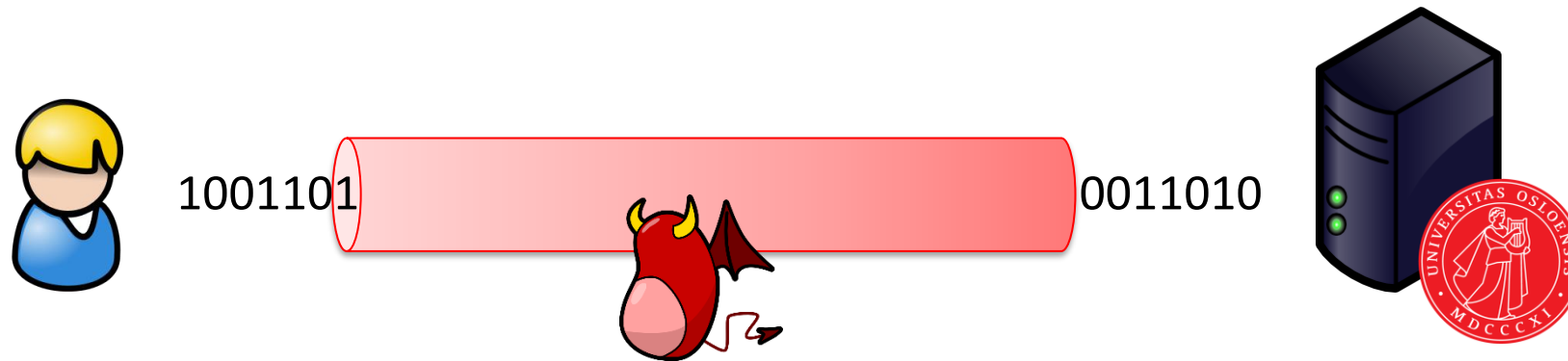
The image shows a web browser window displaying the homepage of the University of Oslo (UiO). The browser's address bar shows the URL <https://www.uio.no>, with a red circle highlighting the lock icon, indicating a secure connection. The page content includes the text "UNIVERSITETET I OSLO" and a promotional message: "Lurer du på hva du «skal bli»? Karriereuka hjelper deg på veien!". Below this message is a link: "→ Besøk Karriereuka". A photograph of a smiling young woman is visible on the right side of the page.

Overlaid on the right side of the browser window is the "Page Info" window for <https://www.uio.no/>. The window has tabs for "General", "Media", "Permissions", and "Security". The "Security" tab is active, showing the following information:

- Website Identity**
 - Website: www.uio.no
 - Owner: This website does not supply ownership information.
 - Verified by: GEANT Vereniging [View Certificate](#)
- 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.
 - [Help](#)

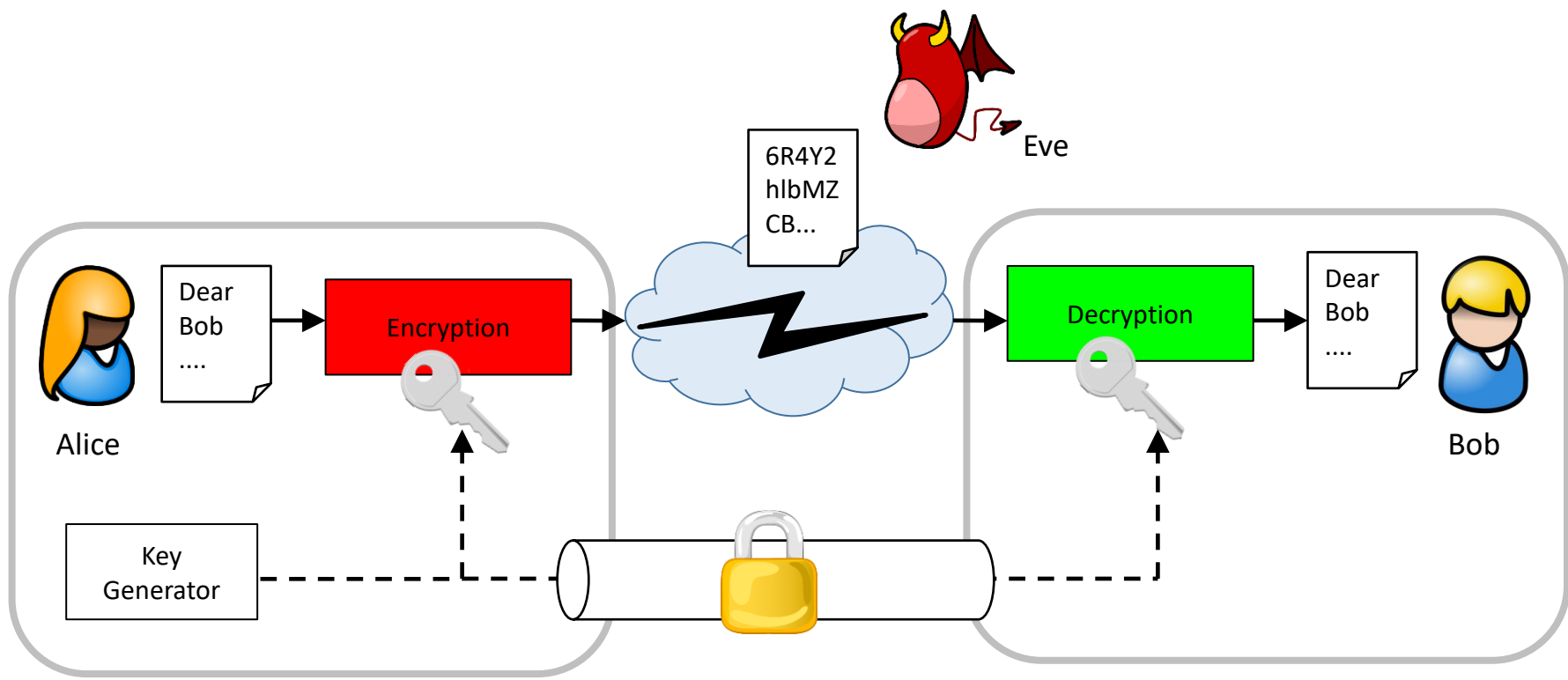
HTTPS / TLS / SSL

- 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

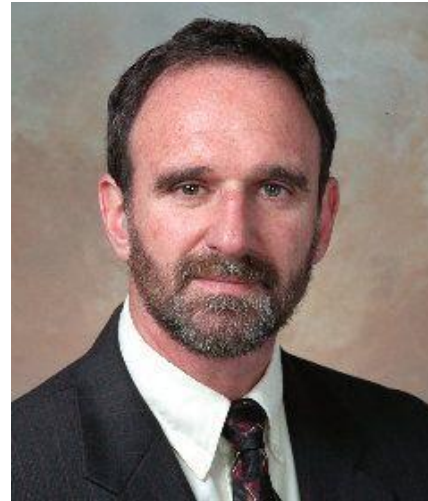
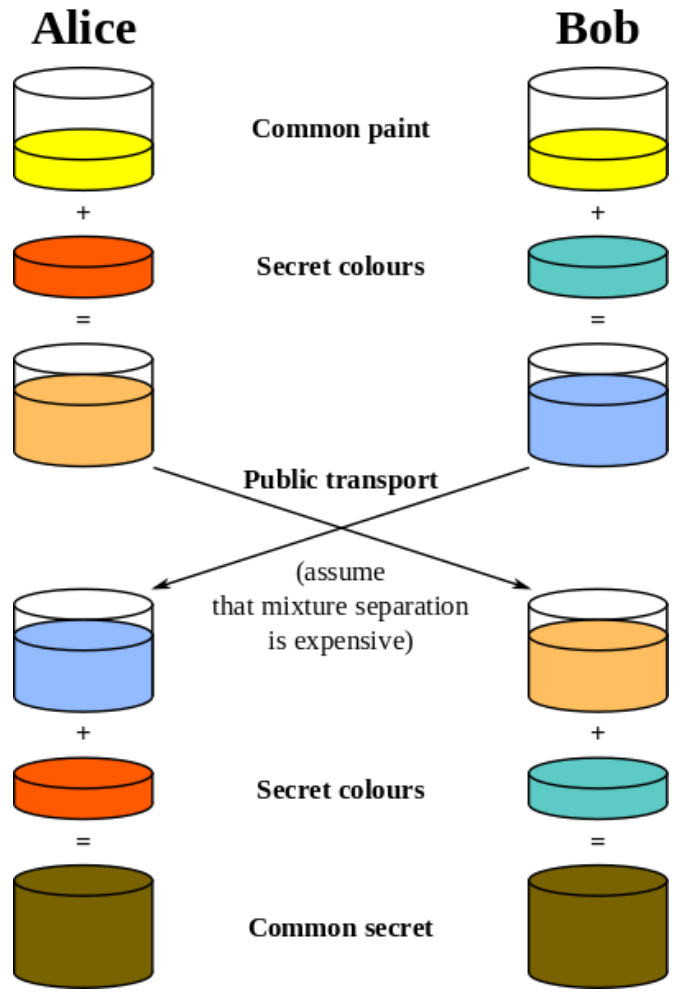
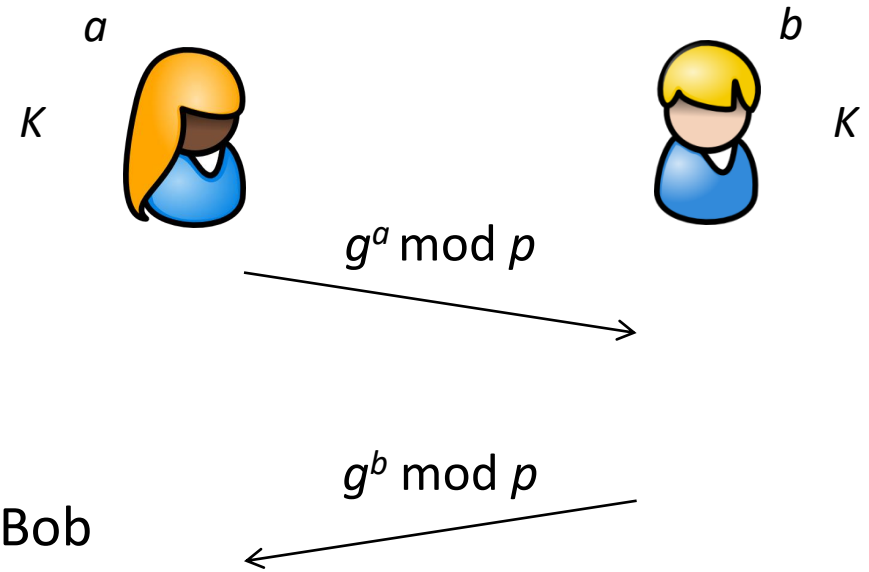


Illustration of DH Key Exchange



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 $g^a \bmod p$ to Bob
- Bob chooses a random number b and send $g^b \bmod p$ to Alice
- Calculation of common secret:
 - Alice: $(g^b)^a \bmod p$
 - Bob: $(g^a)^b \bmod p$
$$\left. \begin{array}{l} \text{Alice: } (g^b)^a \bmod p \\ \text{Bob: } (g^a)^b \bmod p \end{array} \right\} = g^{ab} \bmod p = K$$
- 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



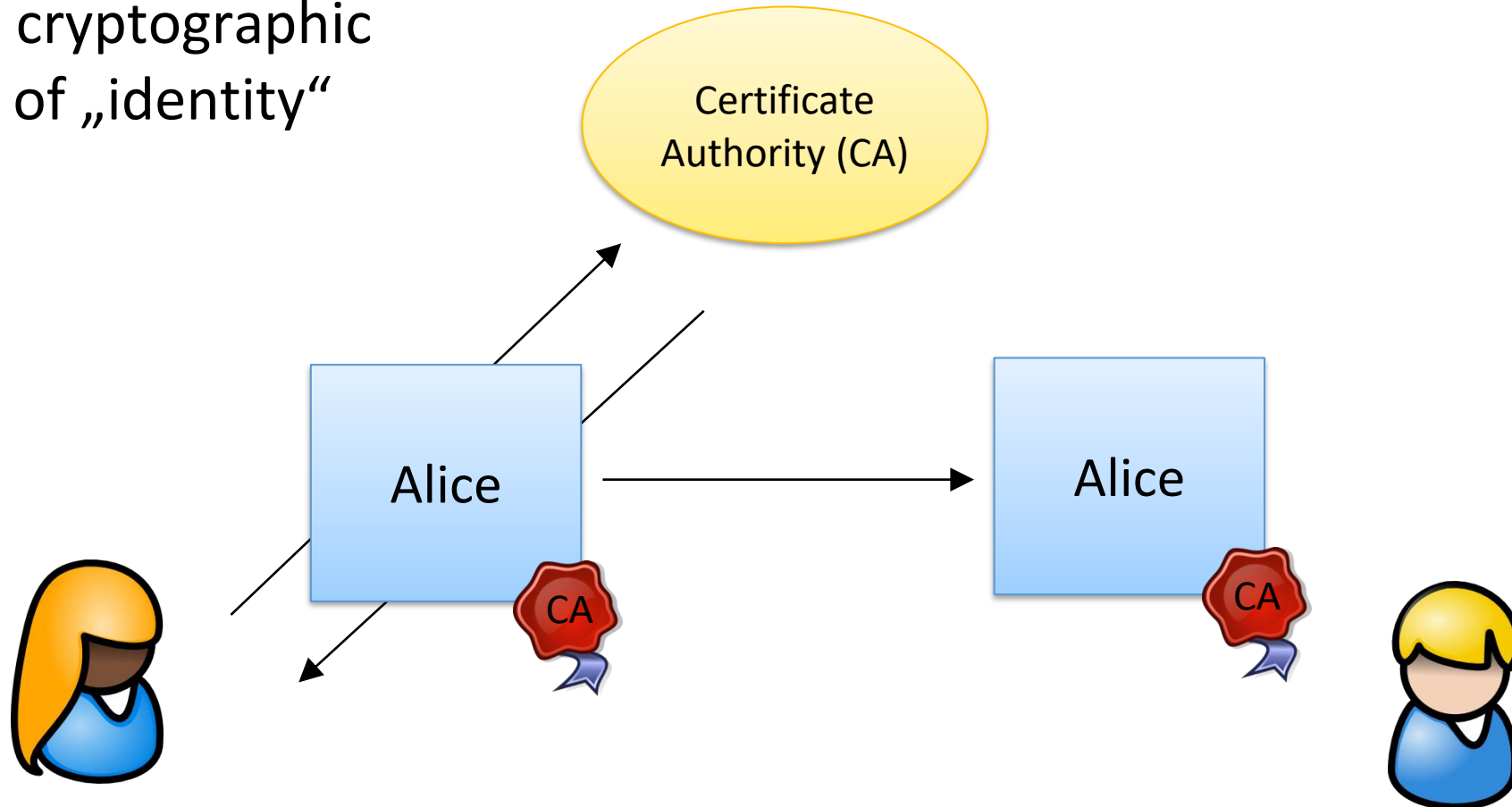
Still a Problem ...

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

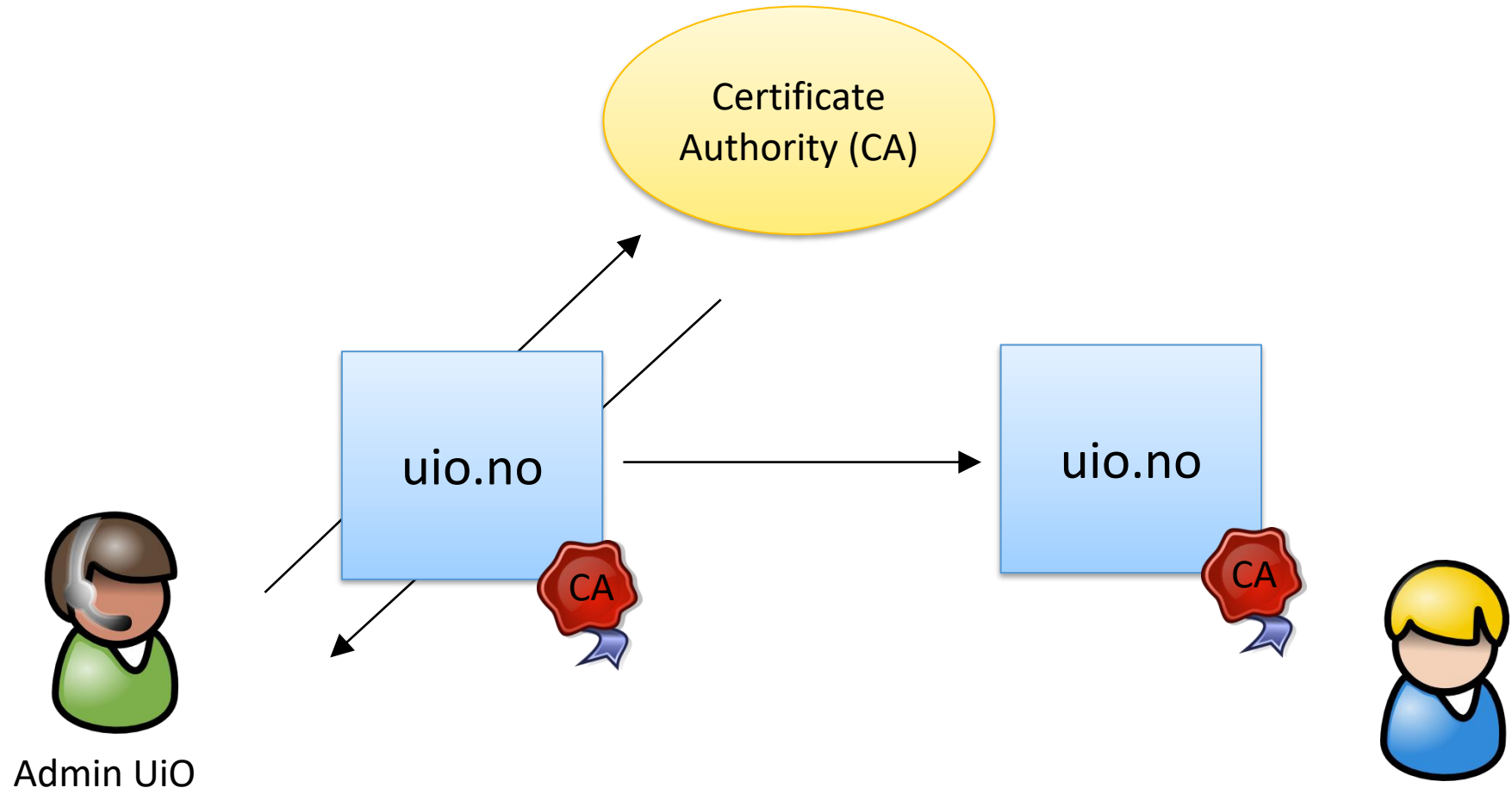


Certificates

- Allow cryptographic proof of „identity“



Certificates



The image shows a browser window with the URL <https://www.uio.no> in the address bar. The page content includes the text "UNIVERSITETET I OSLO" and a promotional message: "Lurer du på hva du «skal bli»? Karriereuka hjelper deg på veien! → Besøk Karriereuka". A red circle highlights the lock icon and the URL in the address bar.

Overlaid on the right is the "Page Info" window for <https://www.uio.no/>. The "Security" tab is active, showing the following details:

- Website Identity**
 - Website: www.uio.no
 - Owner: This website does not supply ownership information.
 - Verified by: GEANT Vereniging [View Certificate](#)
- 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.
 - [Help](#)

UiO : **University of Oslo**

Demonstration

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

Phishing Emails

You have a new personal message from Facebook Services Manager

★ Facebook Services Manager <9posterity@andersonsinc.com>

facebook

from Facebook Services Manager.

ed.

Go to Facebook

@web.de. If you don't want to receive these emails from Facebook in the future,

415 P.O Box 10005 Palo Alto CA 94303

https://www.banglashikhon.com/post/manage/

Date: 01/04/2012

Please click on the link below to open the LinkedIn Message View page:
<http://www.linkedin.com/e/-2ec9-96cc/642d7/ins/458143485/Ann/O'Ryan/EML/?hs=unread&tok=354b6c2d74>

View/reply to this message

Don't want to receive e-mail notifications? [Adjust your message settings](#).

© 2011, LinkedIn Corporation

http://km.ur.ru/postlude.html Ungelesen: 0 Gesamt: 170

Hei.

Din BankID slutter å virke 1 med BankID (med engangs

[Klikk her](#)

Med vennlig hilsen
SpareBank 1

[BankID](#)

BankID er en sikker og enkel identifisering på nett.

www.sparebank1.no

MERK: Du kan ikke svare på denne e-posten.

<https://sniffhusked.com/home/IDLog-on/>

Kjære kunde,

Norwegian Post forteller deg at forsendelses nummeret ditt 98746545 fremdeles venter på instruksjoner fra deg.

Den blir levert så snart kostnadene er betalt.

Gebyrer å betale: 27.27 NOK

Dato: 24.09.2020

[Send Pakken min](#)

Phishing Emails – UiO

From: Message Centre <jiangxn88@hust.edu.cn> ☆
Subject: **Incoming mail rejected**
To: Me <[redacted]@ifi.uio.no> ★

As of 09/08/2019 10:50:00 AM, Web Mail-Client System was unavail
[Update/Recover mails](#)

2019 Webmaster Client ®
IT-Service-Portal

CAS - Central Authentication Service - Mozilla Firefox

CAS - Central Authentication S X +

https://test.baniti.nl/wp-admin/includes/uiio-no/cent

IT Help Desk

Username

Email

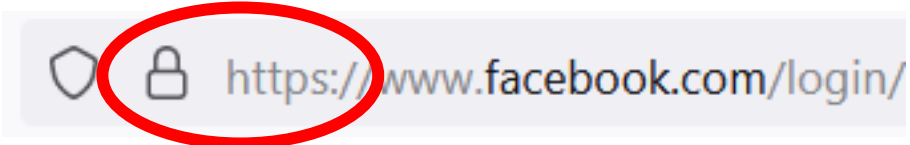
Password

Login

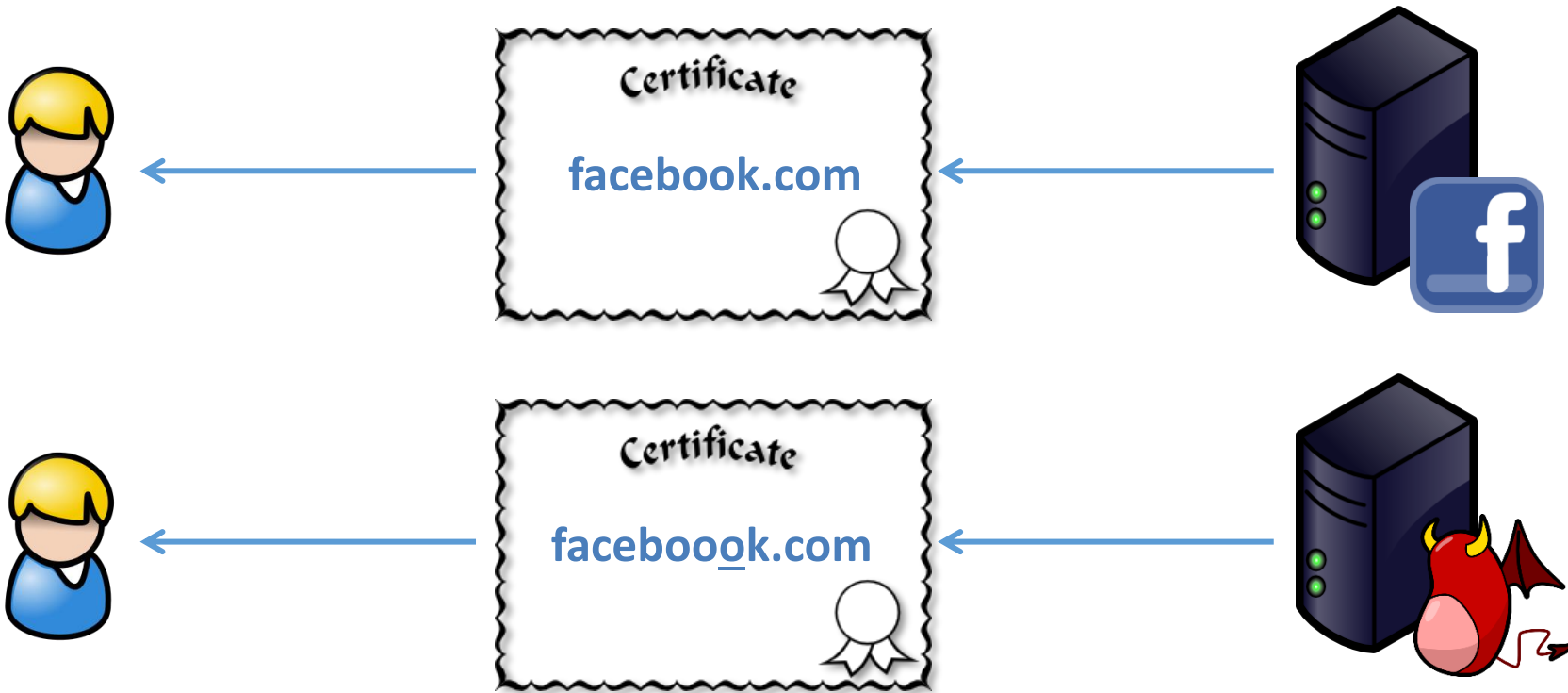
Kindly fill the required information to enable us upgrade your Webmail Account to protect your information against spam, viruses and spyware.

For security reasons, please Log Out and Exit your web browser when you are done accessing services that require authentication!

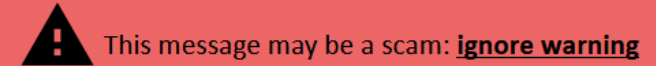
But we used HTTPS ...



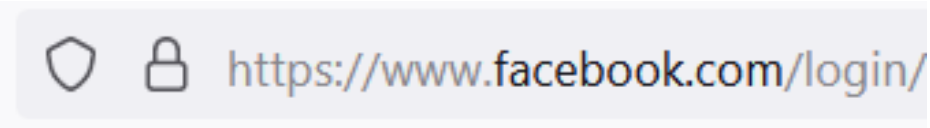
And the Certificate?





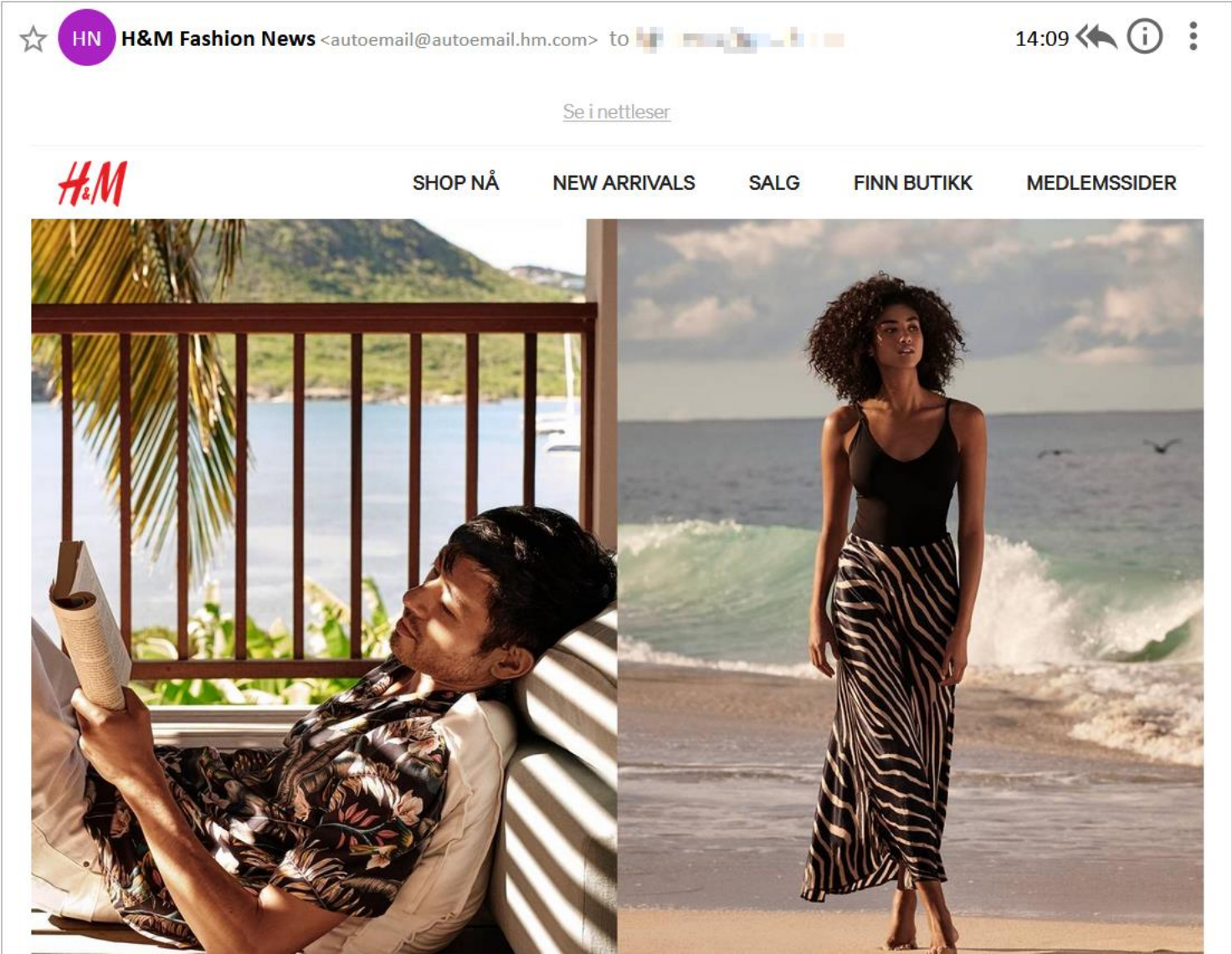
Phishing – Countermeasures



- Some mail programs check for suspicious content
- Observation of To and From addresses (but can be spoofed)
- Careful observation of Web addresses (plus usage of HTTPS/TLS)
- Most important countermeasure: use of common sense!



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



Email Tracking: Images

- Many newsletters contain HTML content:

```
<!DOCTYPE html>
<html style="border:0;margin:0;outline:0;padding:0">
<head>
  <meta http-equiv="content-type" content="text/html; charset=UTF-8">
</head>
<body style="background:#fff;border:0;color:#000;line-height:1;margin:0">
  
```

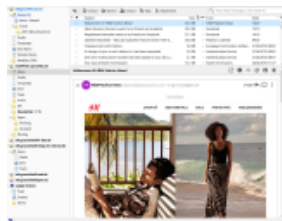
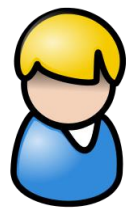

Email Tracking: Images

- Many newsletters contain HTML content:

```
<!DOCTYPE html>  
<html style="border:0;margin:0;outline:0;padding:0">  
<head>  
  <meta http-equiv="content-type" content="text/html; charset=UTF-8">  
</head>  
<body style="background:#fff;border:0;color:#000;line-height:1;margin:0">  
  
```

Email Tracking: Images

- Mail program receives email in HTML format
- HTML document contains image tags (located on Web server of the mail sender)
 - e.g.: ``
- Mail program downloads the images for rendering the HTML mail
- Web server owner (= mail sender) logs the request and can analyze the URL



Email Tracking: Images



- Experiment:
 - Register newsletters with two different email addresses
 - Check the images inside the newsletter
- Newsletter 1:
 - [https://aemcomm.hm.com/content/dam/hm/Seasonal Images Email/Seasonal Images May 2019/e5be3db9-Customer-On-Boarding-3x2-1400x934px.jpg](https://aemcomm.hm.com/content/dam/hm/Seasonal%20Images%20Email/Seasonal%20Images%20May%202019/e5be3db9-Customer-On-Boarding-3x2-1400x934px.jpg)
- Newsletter 2:
 - [https://aemcomm.hm.com/content/dam/hm/Seasonal Images Email/Seasonal Images May 2019/87882c29-Customer-On-Boarding-3x2-1400x934px.jpg](https://aemcomm.hm.com/content/dam/hm/Seasonal%20Images%20Email/Seasonal%20Images%20May%202019/87882c29-Customer-On-Boarding-3x2-1400x934px.jpg)

Email Tracking: Images



- Experiment:
 - Register newsletters with two different email addresses
 - Check the images inside the newsletter
- Newsletter 1:
 - [https://aemcomm.hm.com/content/dam/hm/Seasonal Images Email/Seasonal Images May 2019/e5be3db9-Customer-On-Boarding-3x2-1400x934px.jpg](https://aemcomm.hm.com/content/dam/hm/Seasonal%20Images%20Email/Seasonal%20Images%20May%202019/e5be3db9-Customer-On-Boarding-3x2-1400x934px.jpg)
- Newsletter 2:
 - [https://aemcomm.hm.com/content/dam/hm/Seasonal Images Email/Seasonal Images May 2019/87882c29-Customer-On-Boarding-3x2-1400x934px.jpg](https://aemcomm.hm.com/content/dam/hm/Seasonal%20Images%20Email/Seasonal%20Images%20May%202019/87882c29-Customer-On-Boarding-3x2-1400x934px.jpg)

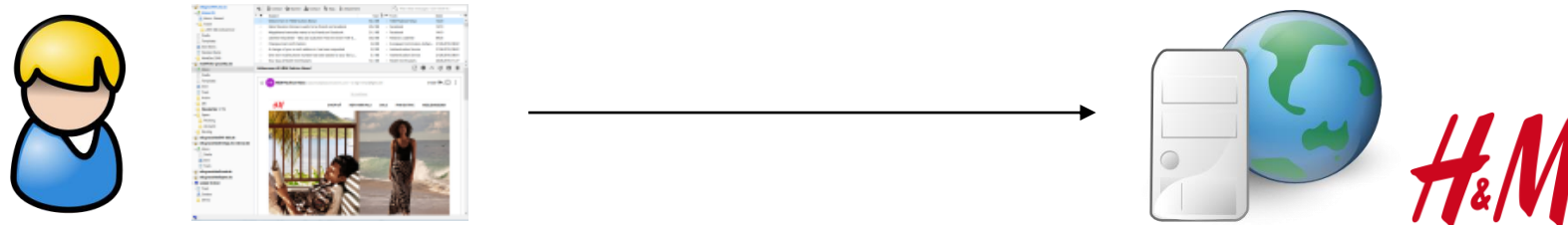
Email Tracking: Images

- Every email address (= user) get different URLs (for the same image)
- Server owner knows when the user has opened the email
- Used for customer relationship management
- Can also be misused for SPAM campaigns:
 - Sender knows that the email is read
 - Send more SPAM messages
 - Sell the email address for a higher price

e5be3db9 = bob@mymail.com

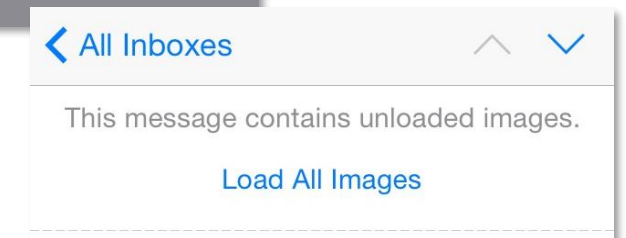
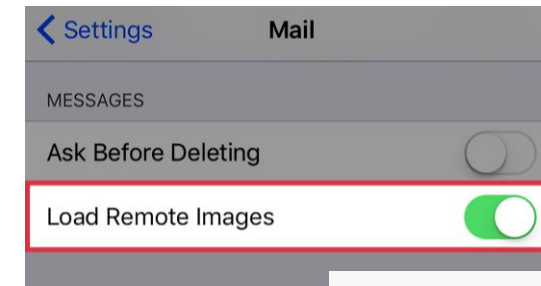
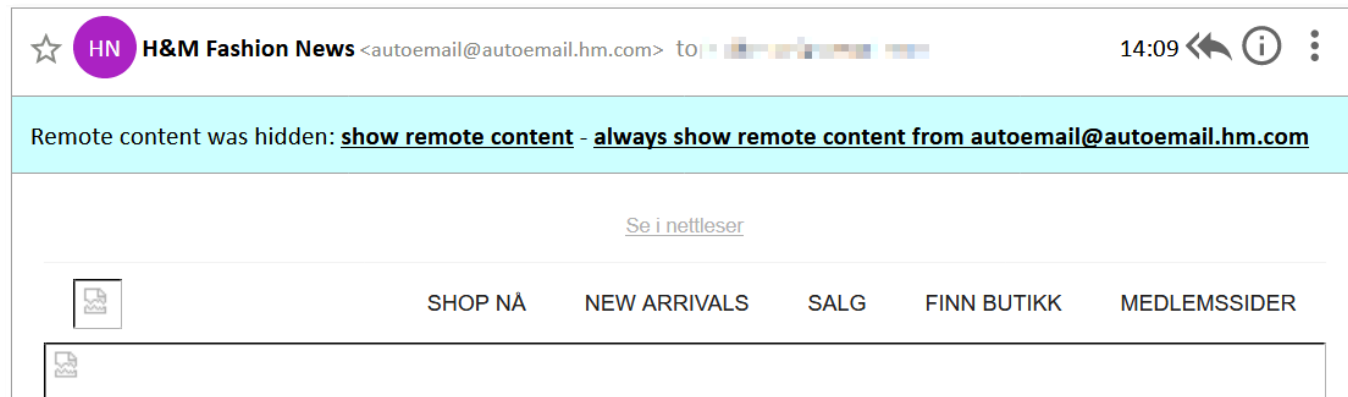
87882c29 = alice@uni.edu.org

...



Email Tracking: Countermeasure

- Configure the email program to not load images in emails (nowadays default in many programs)
- Only load images manually when necessary



Summary

- HTTPS ensures data confidentiality over the Internet
- HTTPS also ensures sender authenticity, i.e., who am I talking to
- 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
- Phishing is still one of the highest threats especially in professional environments