

UiO : **University of Oslo**

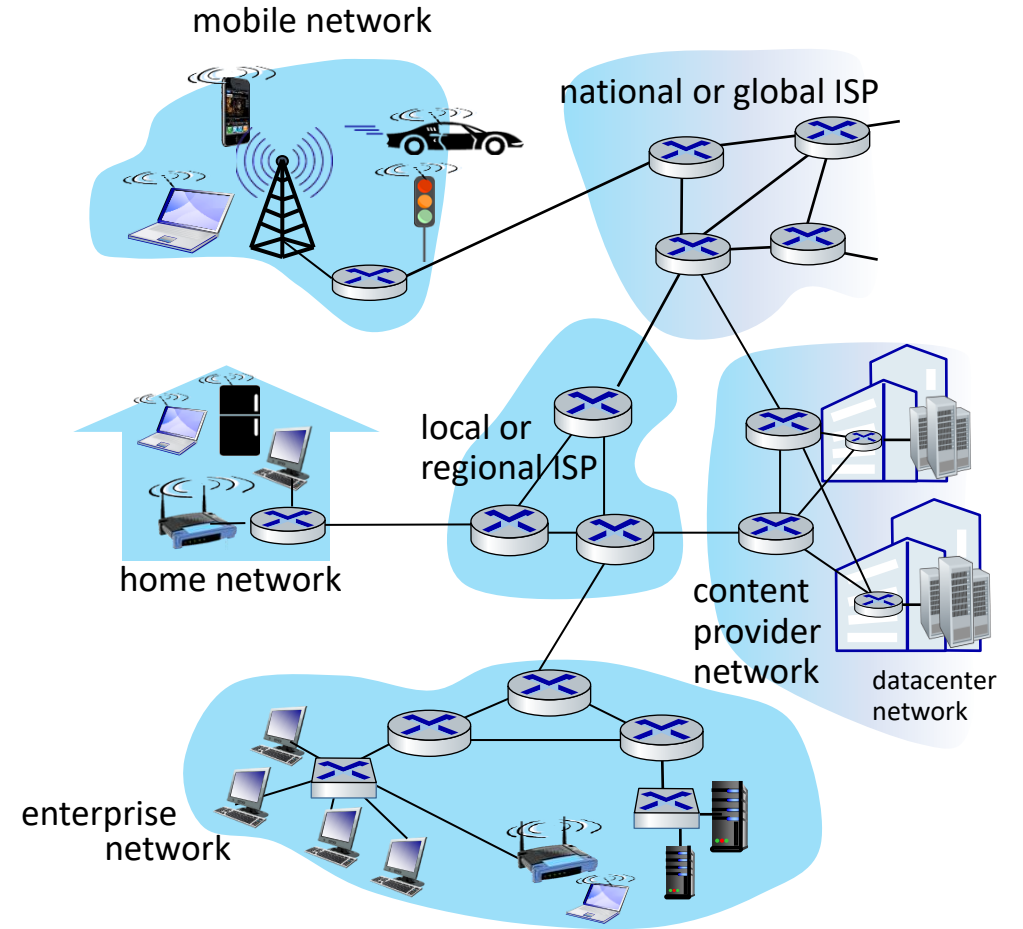
Information technology in the health sector (DIGHEL4360)

Security II – Security for the World Wide Web

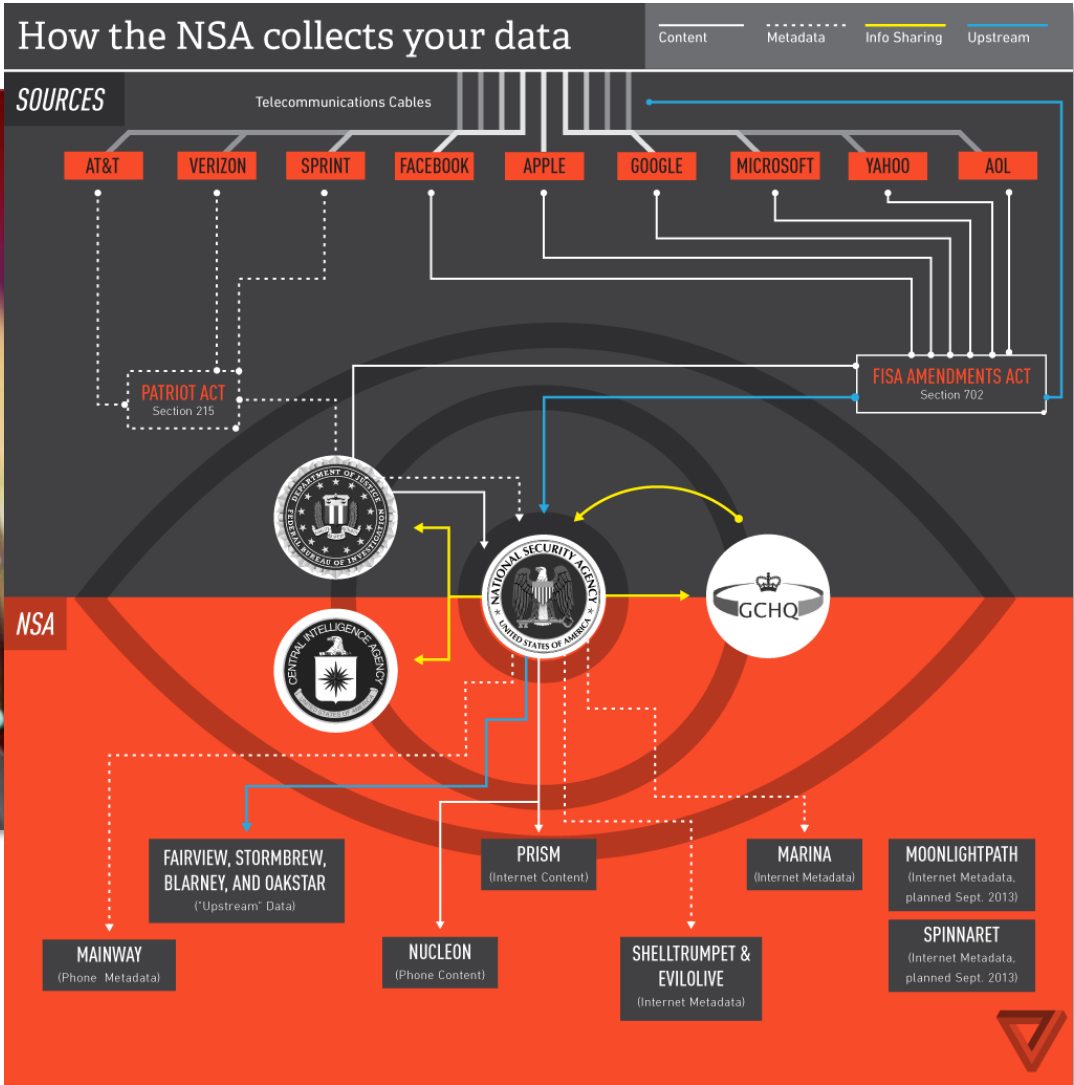


Recapitulation: The Internet

- 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



Why do we need a “more secure Internet”?



Source: <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>
<https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner>

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

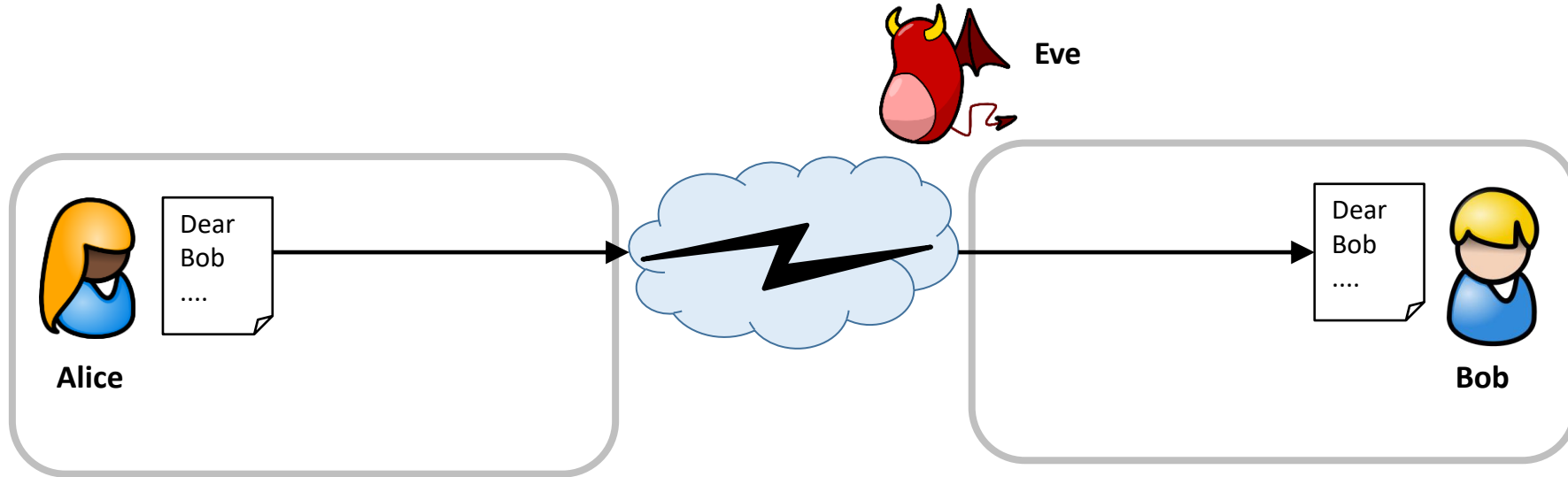
☆

June Bennett

Invoice for Lyd's party photos - Hi Kim, Thanks again for your amazing...

May 6

Confidential Communication

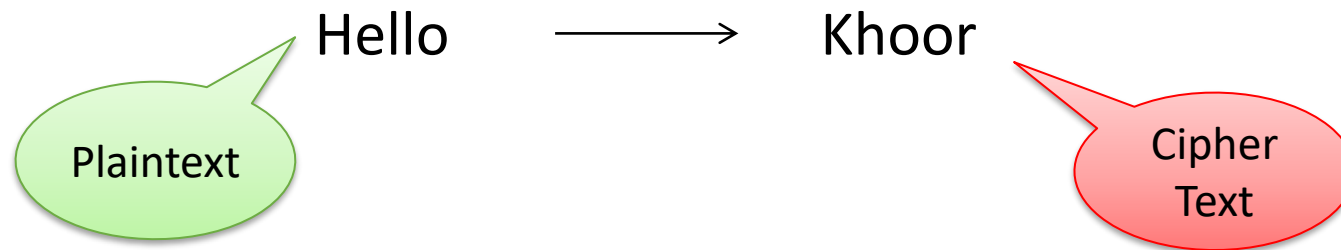
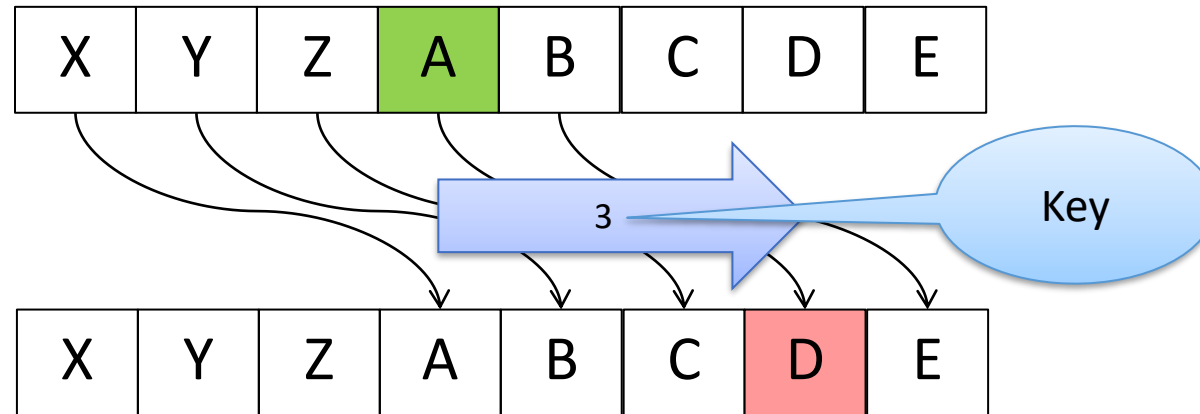


Confidential Communication



Classical Cipher

- Caesar Cipher (50 B.C.)



Encryption

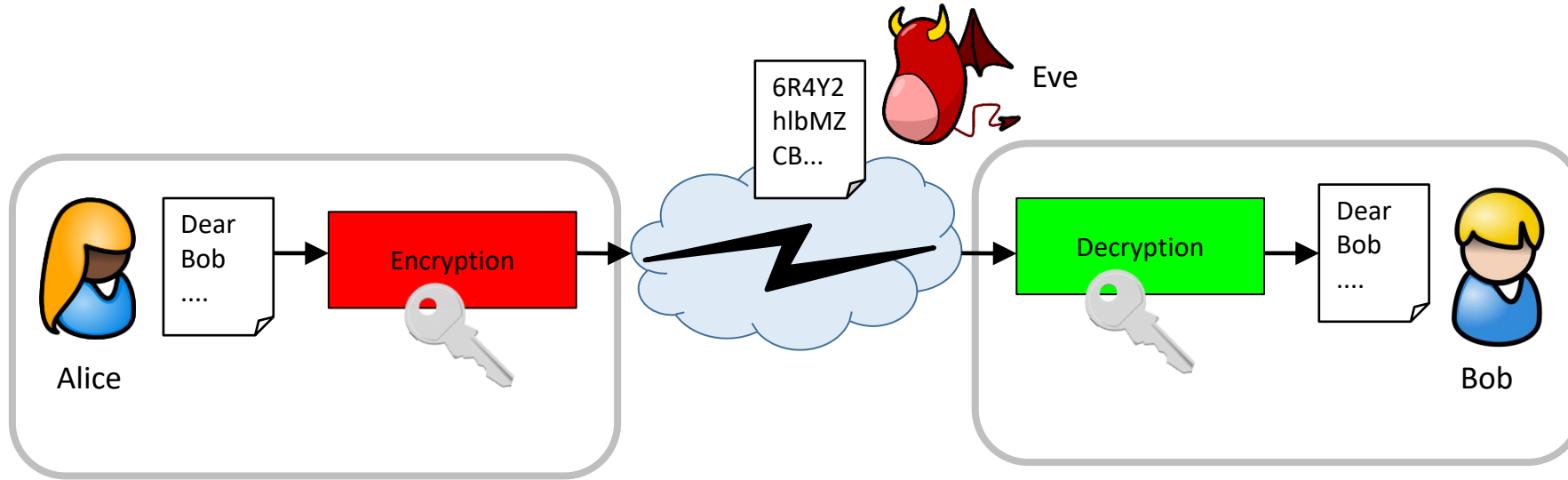
Key = 3



Key = 3



Symmetric Encryption



Caesar Cipher

- Which plaintext is encrypted here?
 - Ymjvznhpgwtbsktcozruxtajwymjqfeditl.
- Try each possible key:
 1. Xliuymgofvsarjsbnyqtwszivxlipedchsk.
 2. Wkhtxlfneurzqiramxpsvryhuwkhodcbgrj.
 3. Vjgswkemtqyphqzlworuqxgtvjgncbafqi.
 4. Uifrvjdlcspxogpykvnqtpwfsuifmbazeph.
 5. Thequickbrownfoxjumpsoverthelazydog.
 6. Sgdpthbjaqnvmenwitlornudqsgdkzyxcnf.
 7. Rfcosgaizpmuldmvhsknqmtcprfcjyxbme.
 8. Qebnrfzhyoltkclugrjmplsboqebixwvald.
 9. Pdamqeygxnsjbktfqilokranpdahwvuzkc.
 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



Geheime Kommandosache! Jede einzelne Tageschlüssel ist geheim. Mitnehmen im Flugzeug verboten!

Nr. 00190

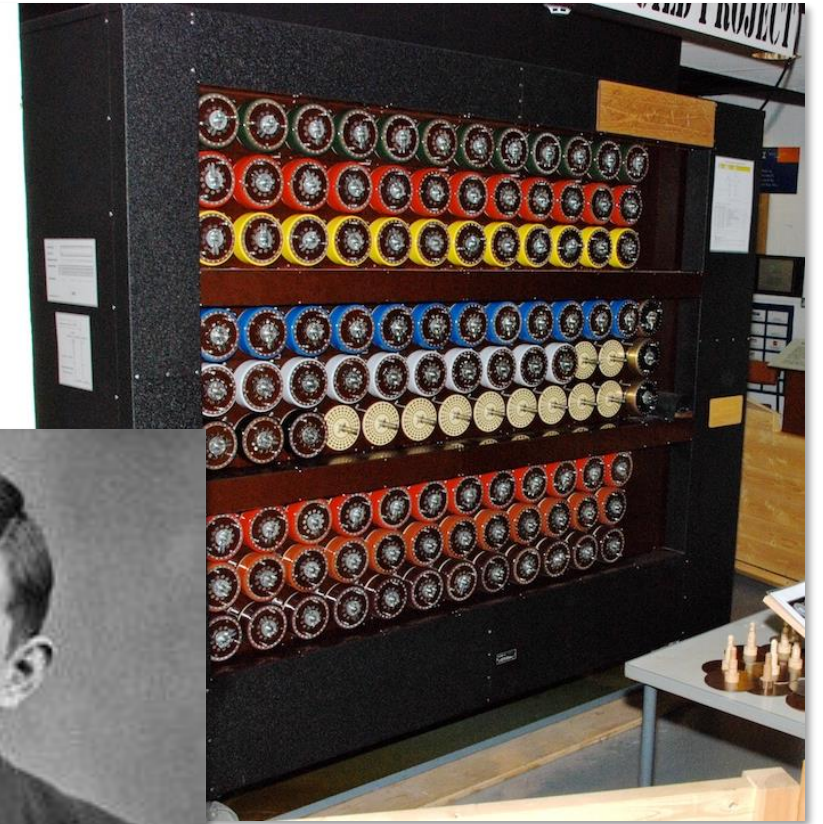
Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Monats- tag	Wellenlage				Ringstellung	S i e d i v e r b i n d u n g e n										Kenngruppen				
						an der Umkehrmole		am Stecherbrett												
								1	2	3	4	5	6	7	8	9	10			
049	31	I	V	III	14 09 24			SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ekb rzg
049	30	IV	III	II	05 26 02			IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	kti	acw	zsi wao
049	29	III	II	I	12 24 03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	PZ	fn	acn	ovw wvd
049	28	II	III	V	06 08 16	DI	CN	BR	PV	CR	FV	AI	DK	OT	MQ	EU	BX	LP	GJ	ude rzh
049	27	III	I	IV	11 03 07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	PP	HT	EX	UW	vct uis
049	26	I	IV	V	17 22 19			VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev rxm
049	25	IV	III	I	08 25 12			OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew uit
049	24	V	I	IV	05 18 14			TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci tlg
049	23	IV	II	I	24 12 04			QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn	rwm	udf tlo
049	22	II	IV	V	01 09 21	IU	AS	DV	OL	FJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jac acx
049	21	I	V	II	13 05 19	PT	OX	EZ	CH	RU	HL	FY	OS	GZ	DM	AW	CE	TV	NX	jpw del
049	20	III	IV	V	24 01 10	MR	KN	BQ	PW	DF	MO	QZ	AU	RY	SV	JL	GX	BE	TW	jqd cef
049	19	V	III	I	17 25 20			OX	PR	PH	WY	DL	CM	AE	TZ	JS	GI	idf	fx	jwg tlg
049	18	IV	II	V	15 23 26			EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	bw	vcj rxn
049	17	I	IV	II	21 10 06			IR	KZ	LS	EM	OV	OY	QX	AP	JP	BU	mae	hzi	sog ysi
049	16	V	II	III	08 16 13			HM	JO	DI	NR	BY	XZ	GS	PU	PQ	CT	tdp	dhb	fkf uiv
049	15	II	IV	I	01 03 07			DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh wvg
049	14	IV	I	V	15 11 05	AI	BT	MV	HU	GM	JR	KS	IY	HZ	PL	AX	BT	cq	nv	imz noa
049	13	I	III	II	13 20 03	PW	EL	DG	KN	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr dgz
049	12	V	I	IV	18 10 07	RZ	OQ	CP	SX	MU	BP	CY	RZ	KX	AN	JT	DG	IL	PW	zdy rkf
049	11	II	IV	III	02 26 15			KN	UY	HR	PW	FM	BO	EZ	QT	DX	JV	zea	rjy	soi wvh
049	10	III	V	IV	23 21 01			LR	IK	MS	QU	HW	PT	GO	VX	PZ	EN	lrc	zbx	vbm rxo
049	9	V	I	III	16 04 08			QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj	eyr	vby tih
049	8	IV	II	V	13 19 25			FI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz	dha	ekc tli
049	7	I	IV	II	09 03 22			UX	IZ	HN	BK	OQ	CP	FT	JY	MW	AR	lan	dgb	zsj wbi
049	6	III	I	V	11 18 14			DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft	zsk wbj
049	5	V	II	IV	23 02 25	IL	AP	EU	HO	MV	CL	OK	OQ	BI	FU	HS	PX	NW	EY	lju cdr
049	4	II	IV	I	04 21 09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	OP	SU	DH	JM	TX	lsb zby
049	3	V	I	II	19 11 06	BF	NR	DX	CS	KR	MP	CN	BP	EH	DZ	IW	AV	GJ	LO	lap owd
049	2	IV	V	I	16 14 02			BN	HU	EG	PY	KQ	CP	OS	JW	AI	VZ	aqd	bdy	iyf xtd
049	1	II	I	III	23 12 10			DP	BM	NZ	CK	GV	HQ	AP	UY	SW	JO	kgi	cdf	giq wuv

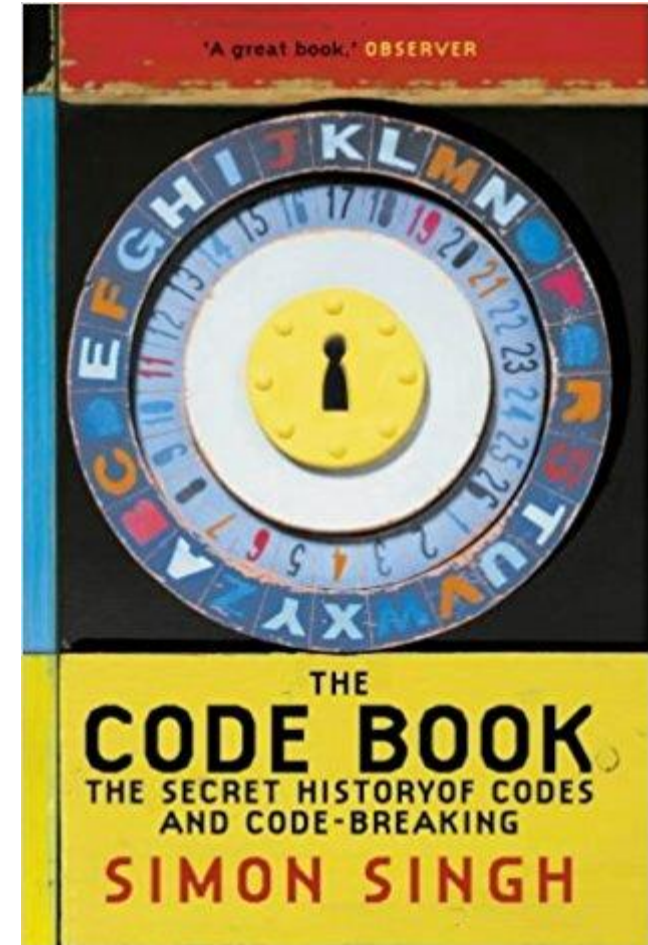
Enigma

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



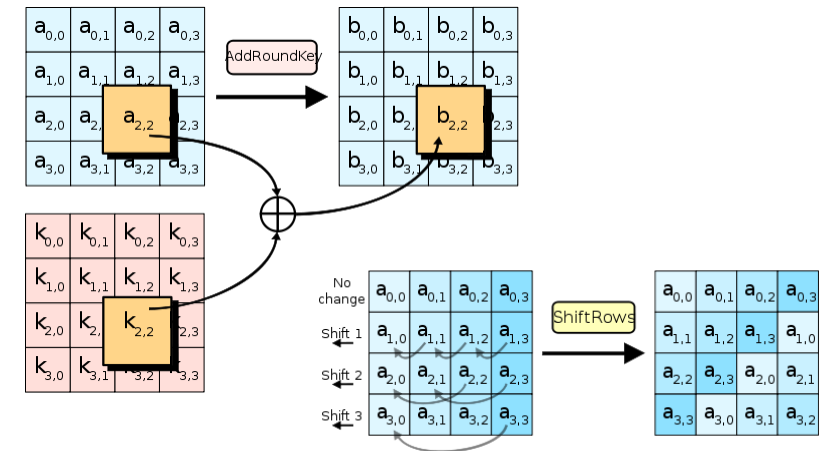
History of Cryptography

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

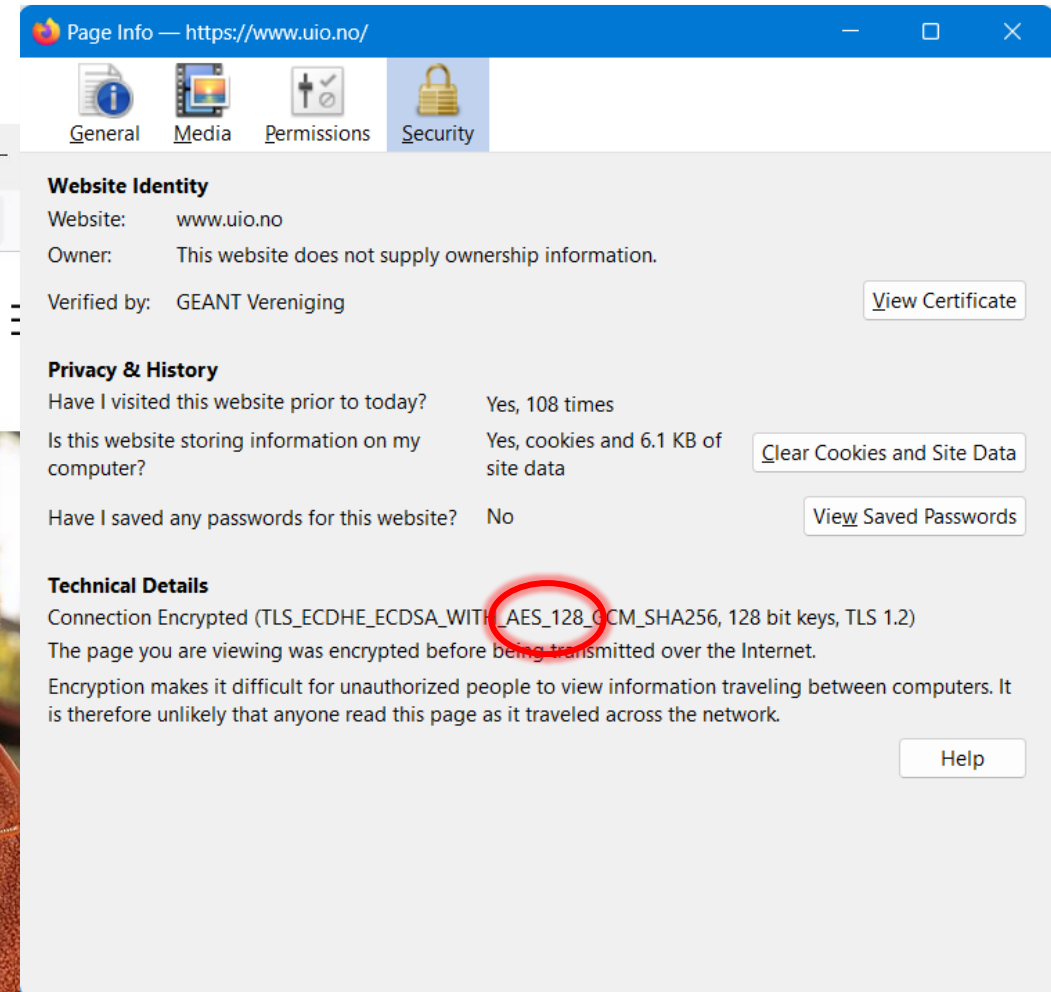
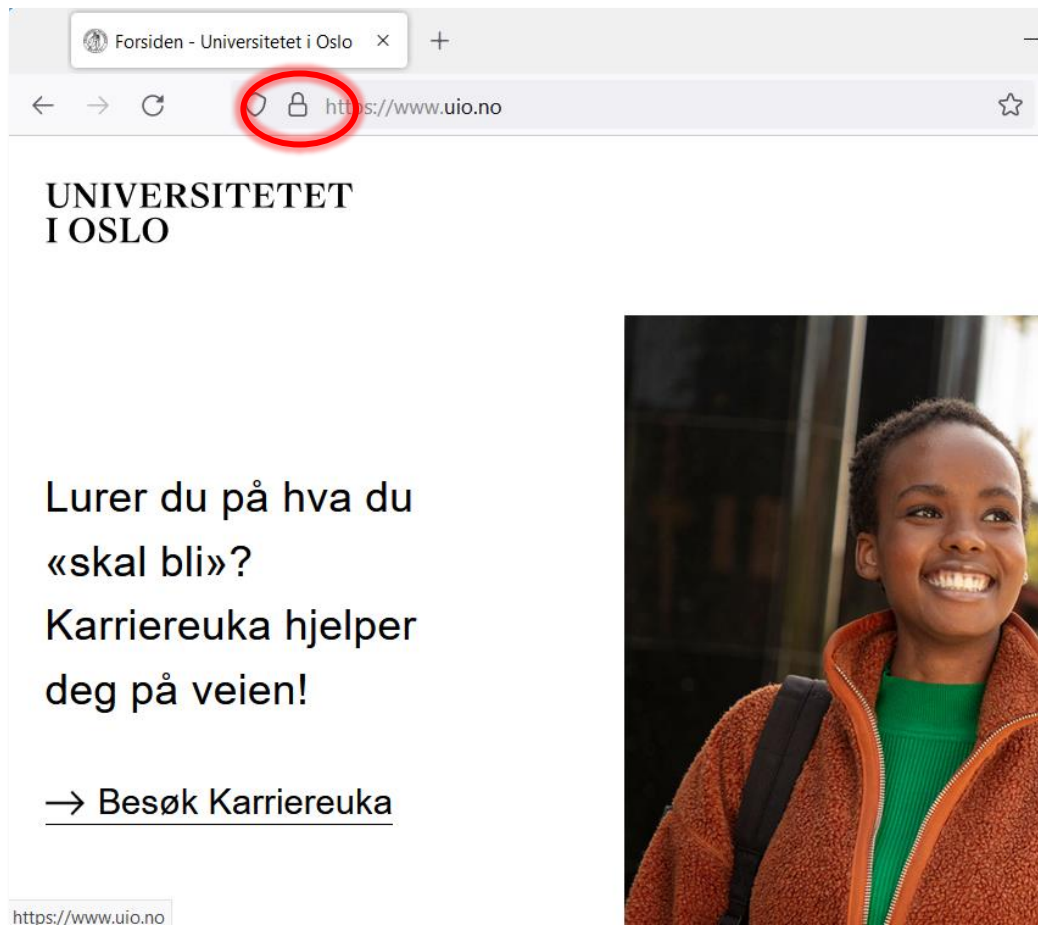


Modern symmetric Encryption

- 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 (≈ 32 letters)
- Brute force attack on 128 or 256 bit key?
(Assumption: breaking 56 bit in 1 second
→ in reality more)

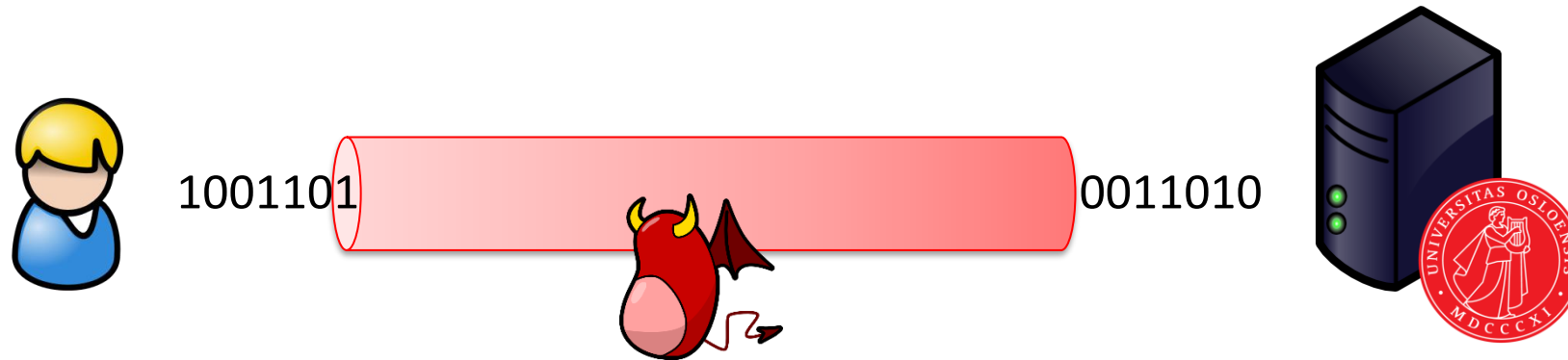


Key length	Duration
56 bit	1 s
64 bit	4 m
80 bit	194 d
112 bit	10^9 a
128 bit	10^{14} a
192 bit	10^{33} a
256 bit	10^{52} a



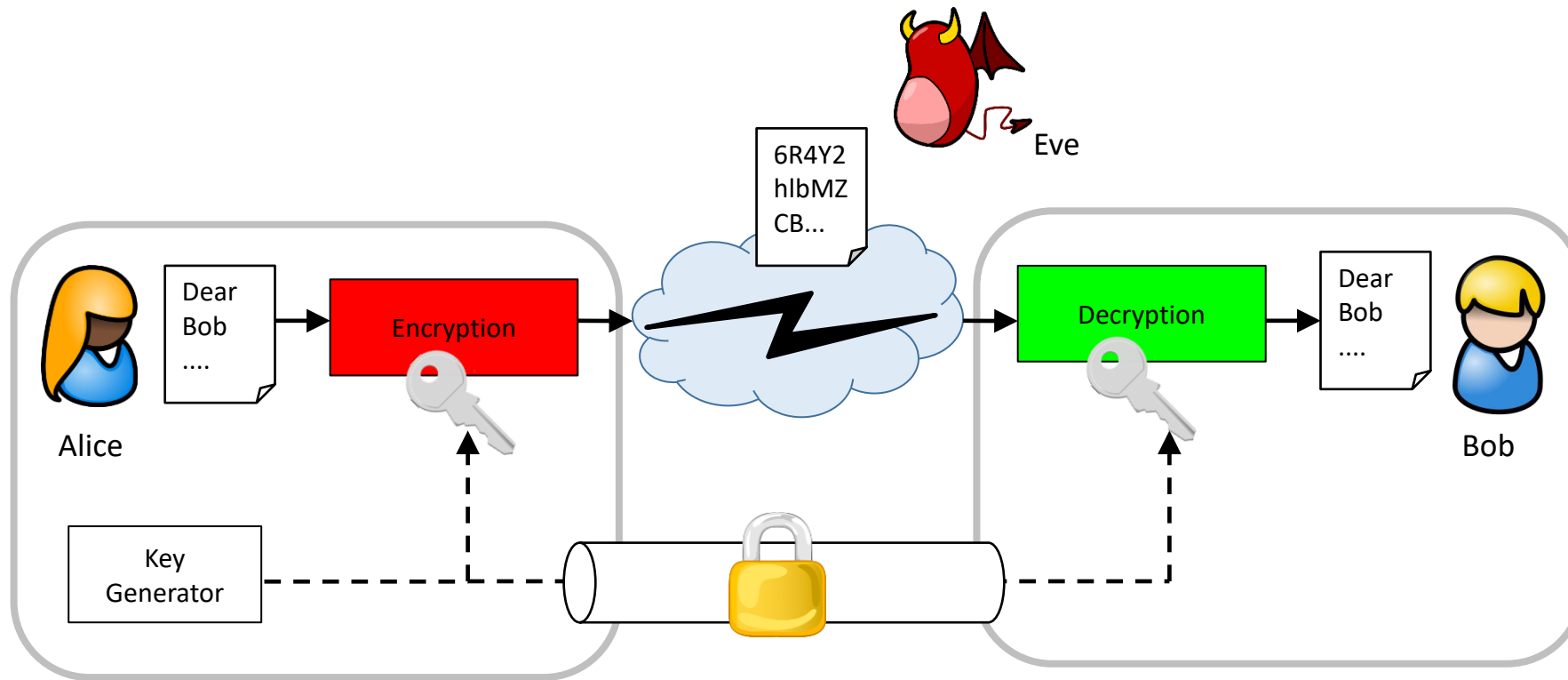
HTTPS / TLS / SSL

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



Symmetric Encryption

- Remaining problem: key exchange

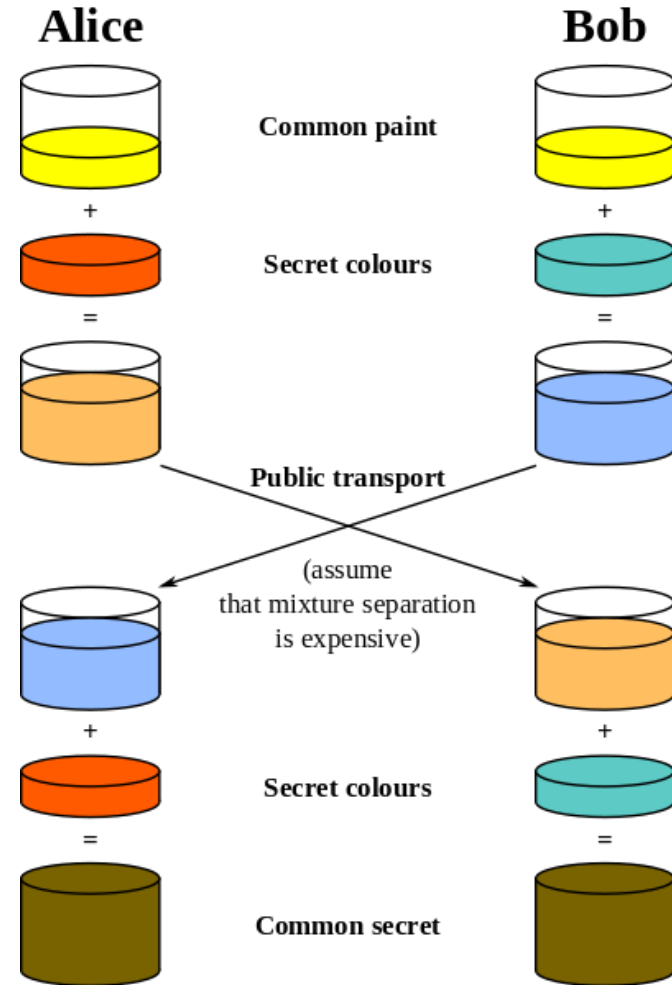


Diffie Hellman Key exchange

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

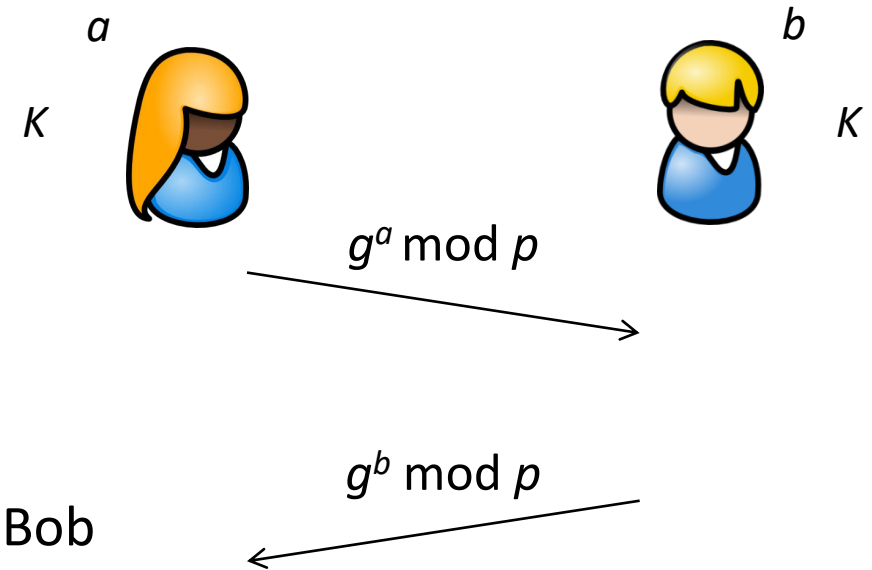


Illustration of DH Key Exchange



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



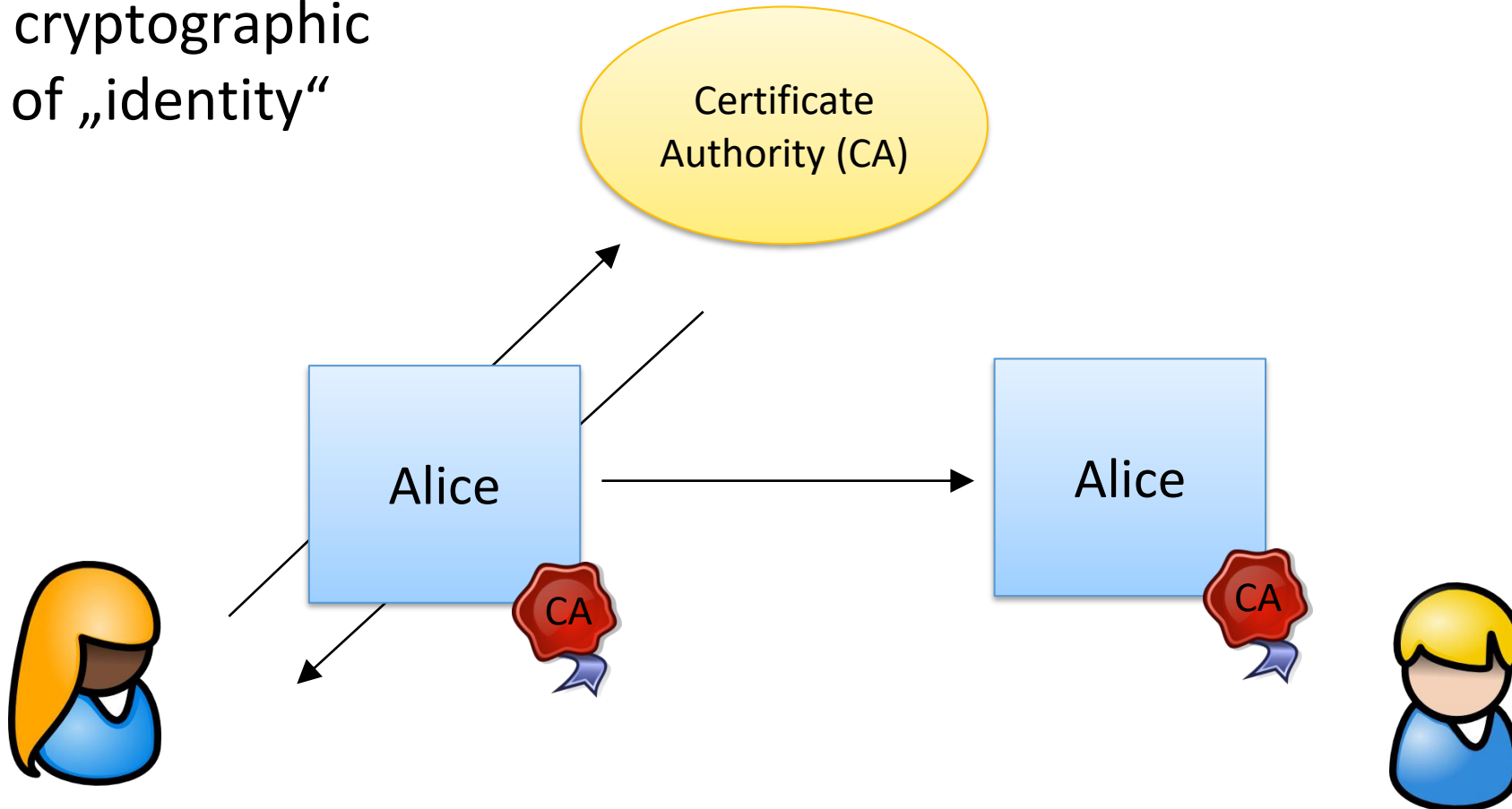
Still a Problem ...

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

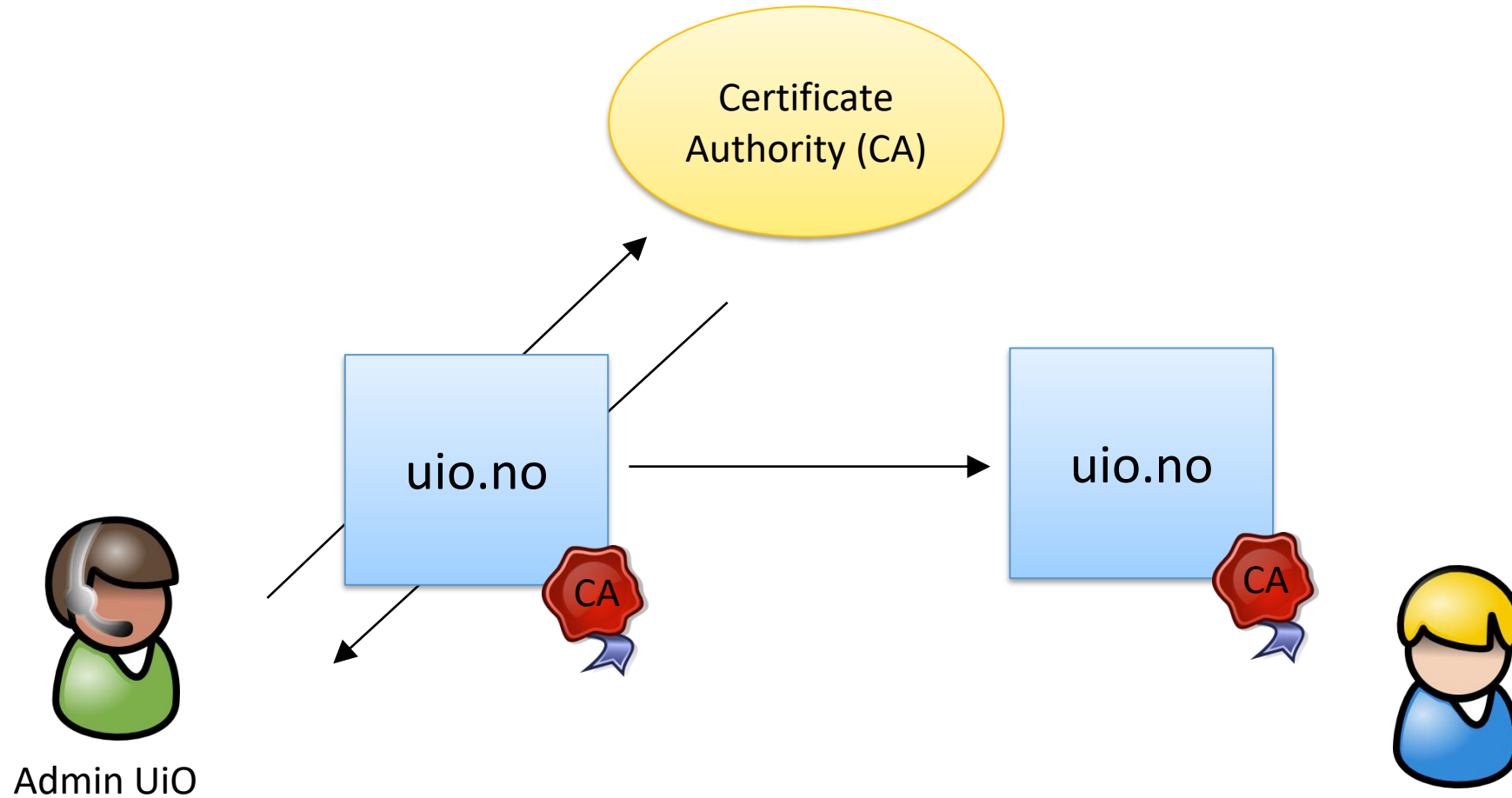


Certificates

- Allow cryptographic proof of „identity“



Certificates

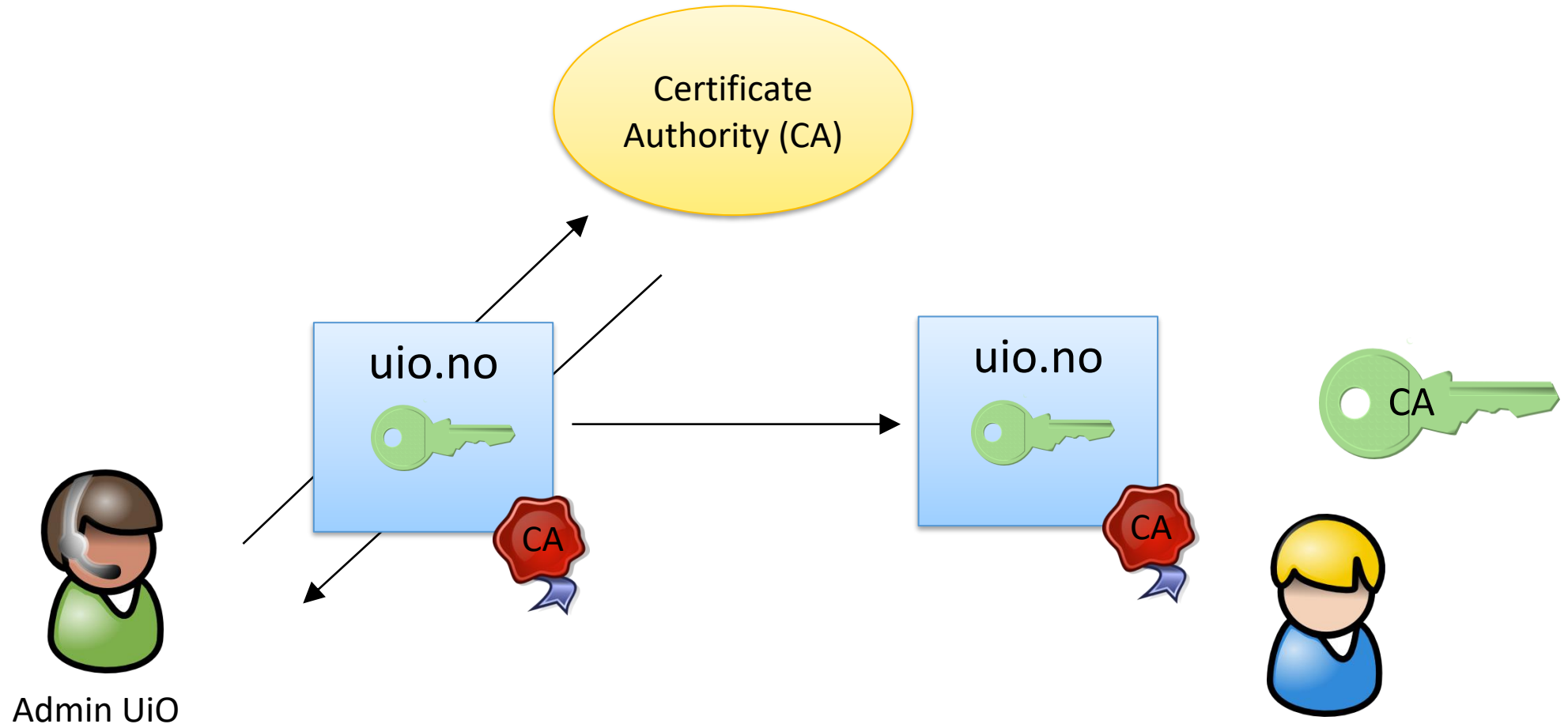


Certificates – more technical

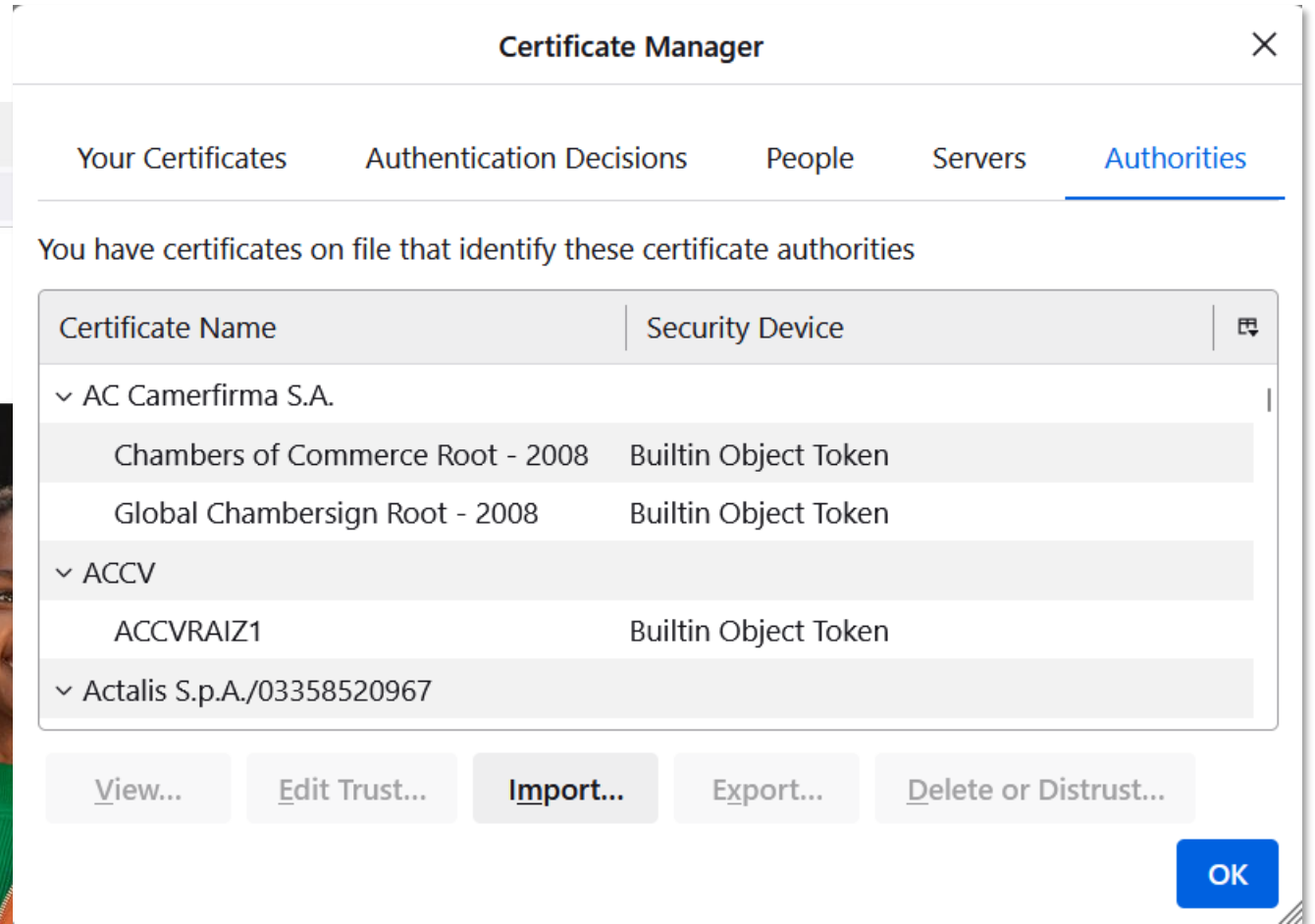
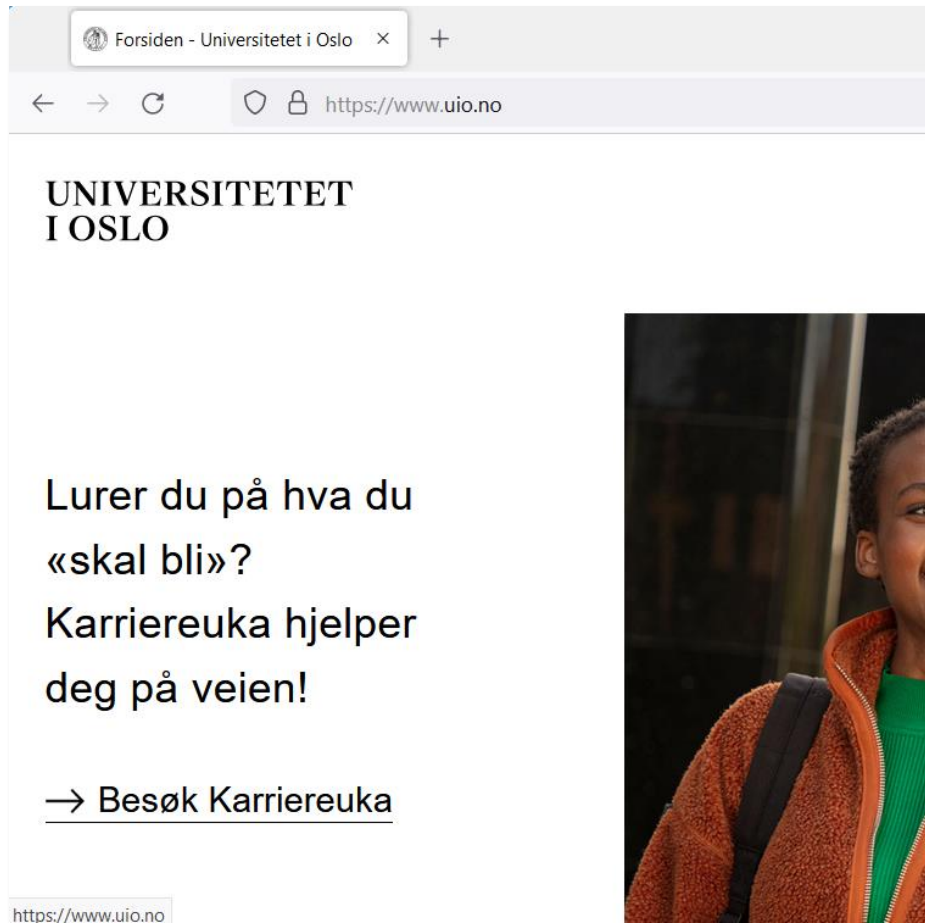


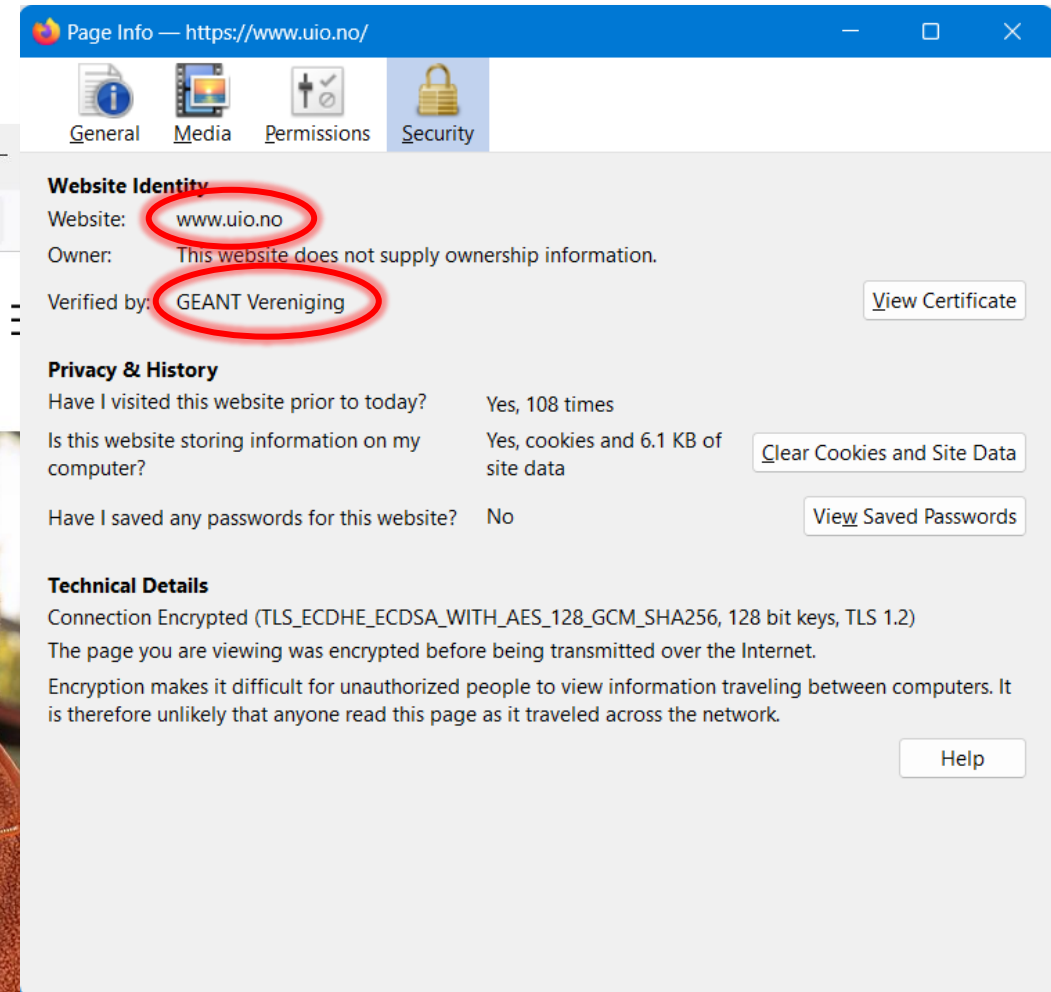
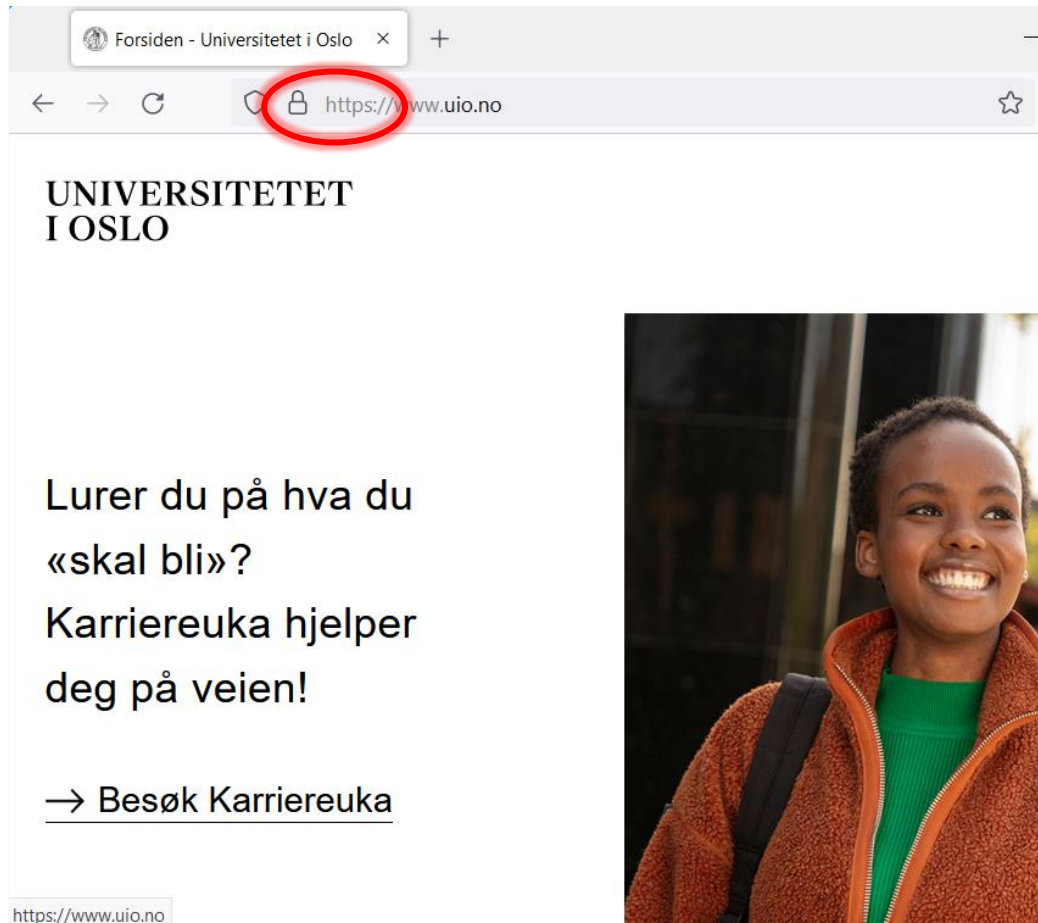
- The certificate contains:
 - An identifier (host name of the Web server)
 - A *cryptographic (public) key*
- The CA creates a *digital signature* that
 - certifies that the CA has verified the identity of the “subject” (here: uio.no)
- The recipient of a digital signature:
 - must *verify* that the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

Certificates



Trusted Certificates built-in in the browser





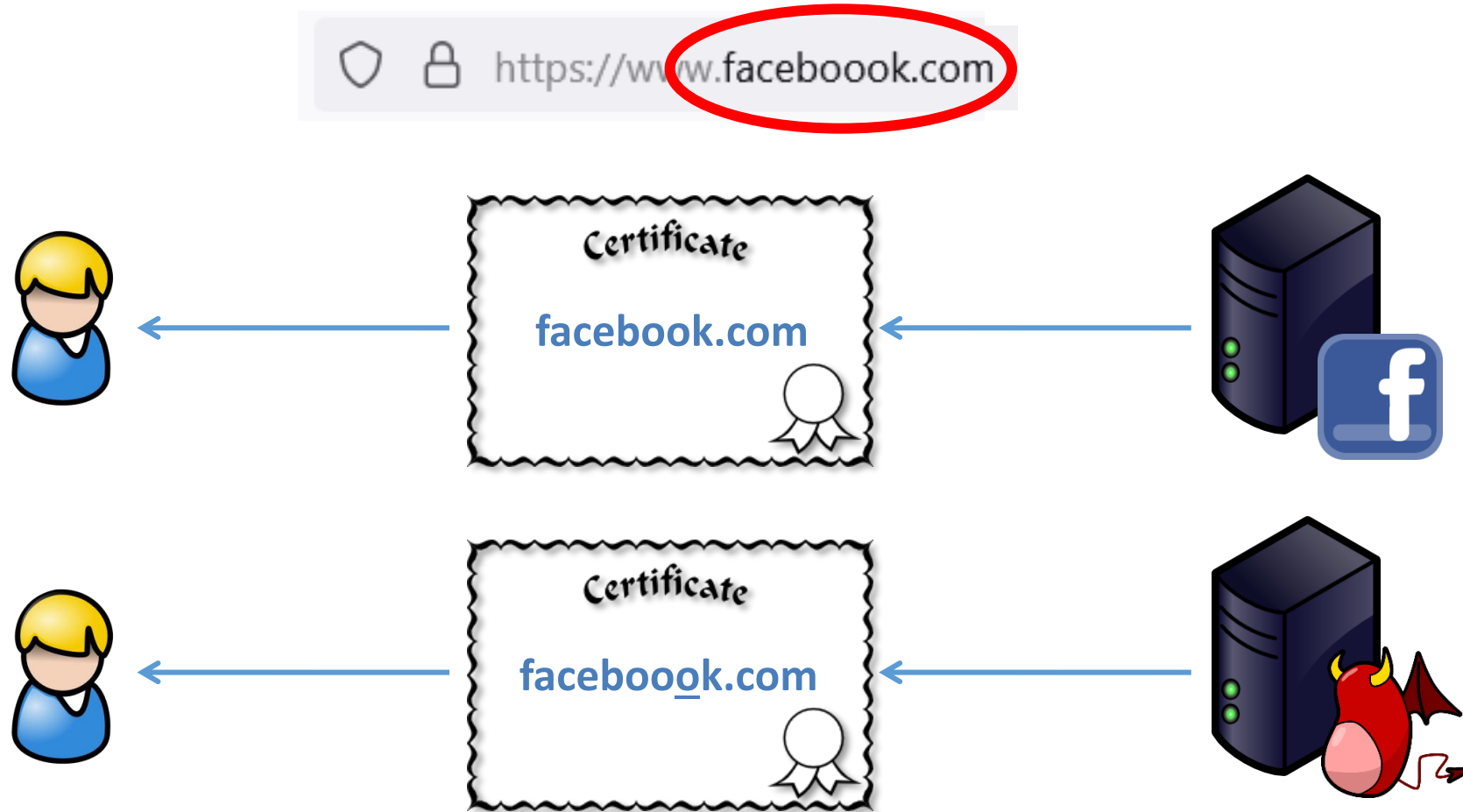
Phishing

- 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 ...

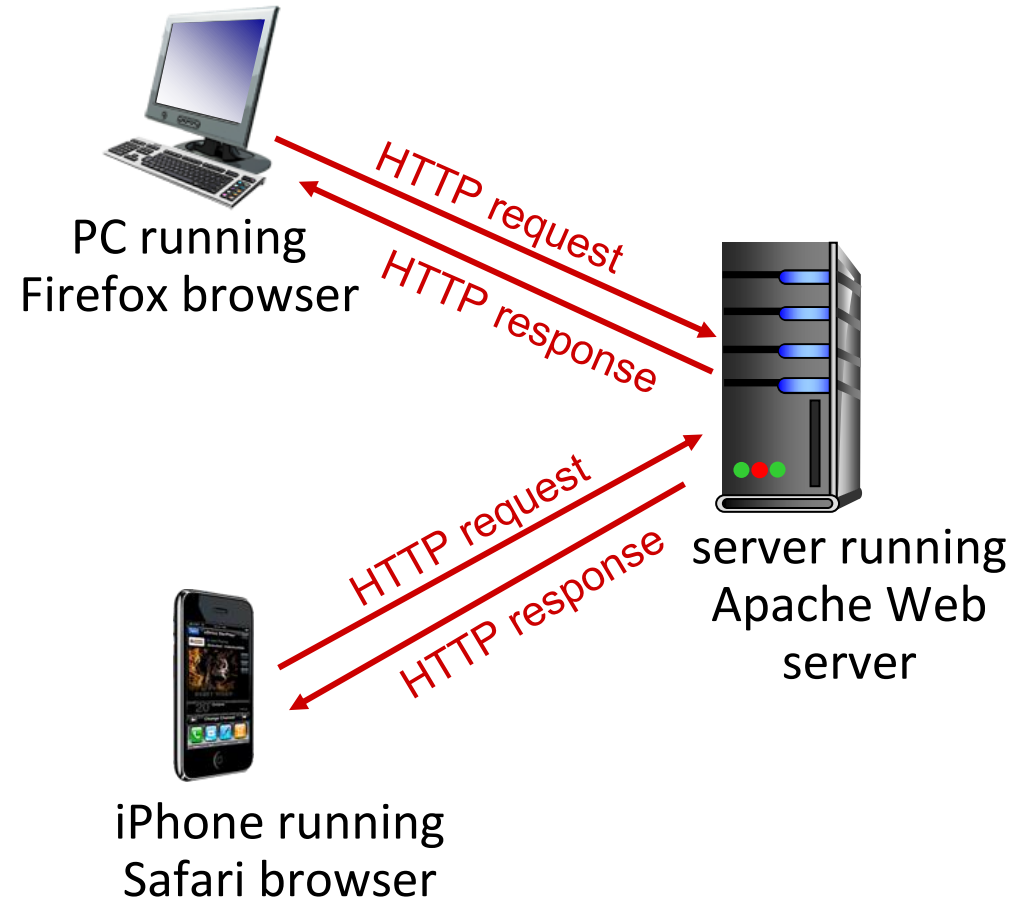


And the Certificate?



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



HTTP Request Message

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

Request line (GET, POST,
HEAD commands)

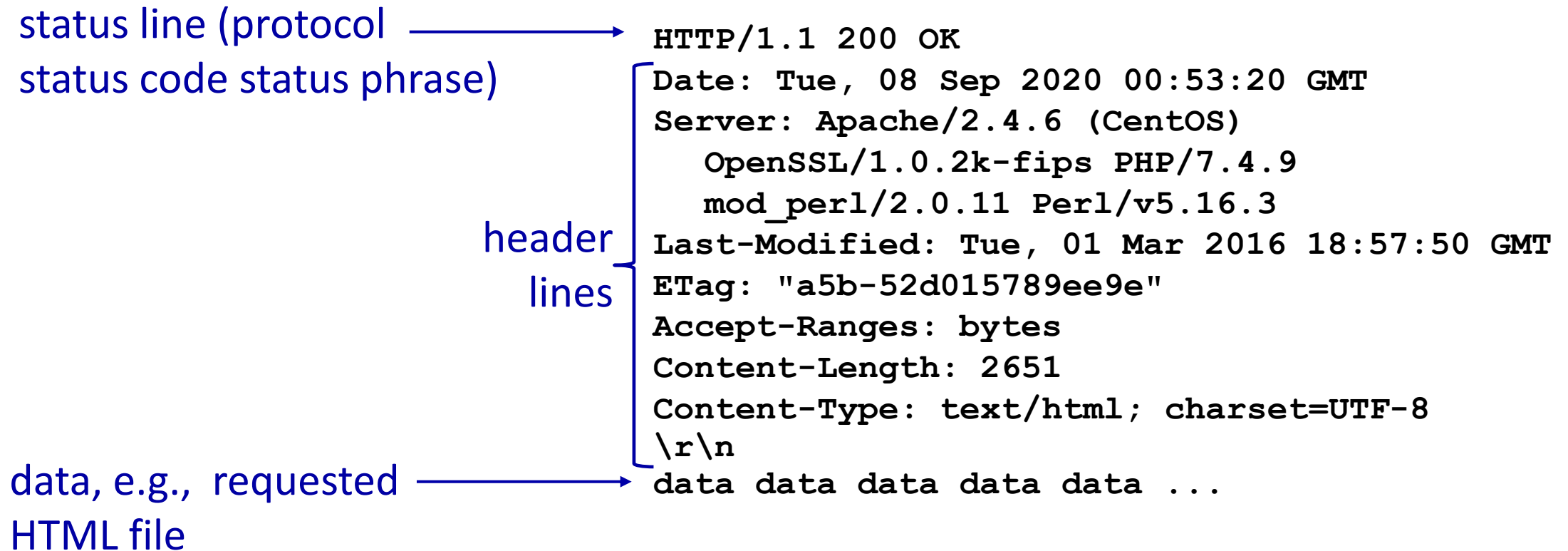
header
lines

```
GET /index.html HTTP/1.1\r\n
Host: www-net.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10.15; rv:80.0) Gecko/20100101 Firefox/80.0 \r\n
Accept: text/html,application/xhtml+xml\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Connection: keep-alive\r\n
\r\n
```

carriage return character
line-feed character

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

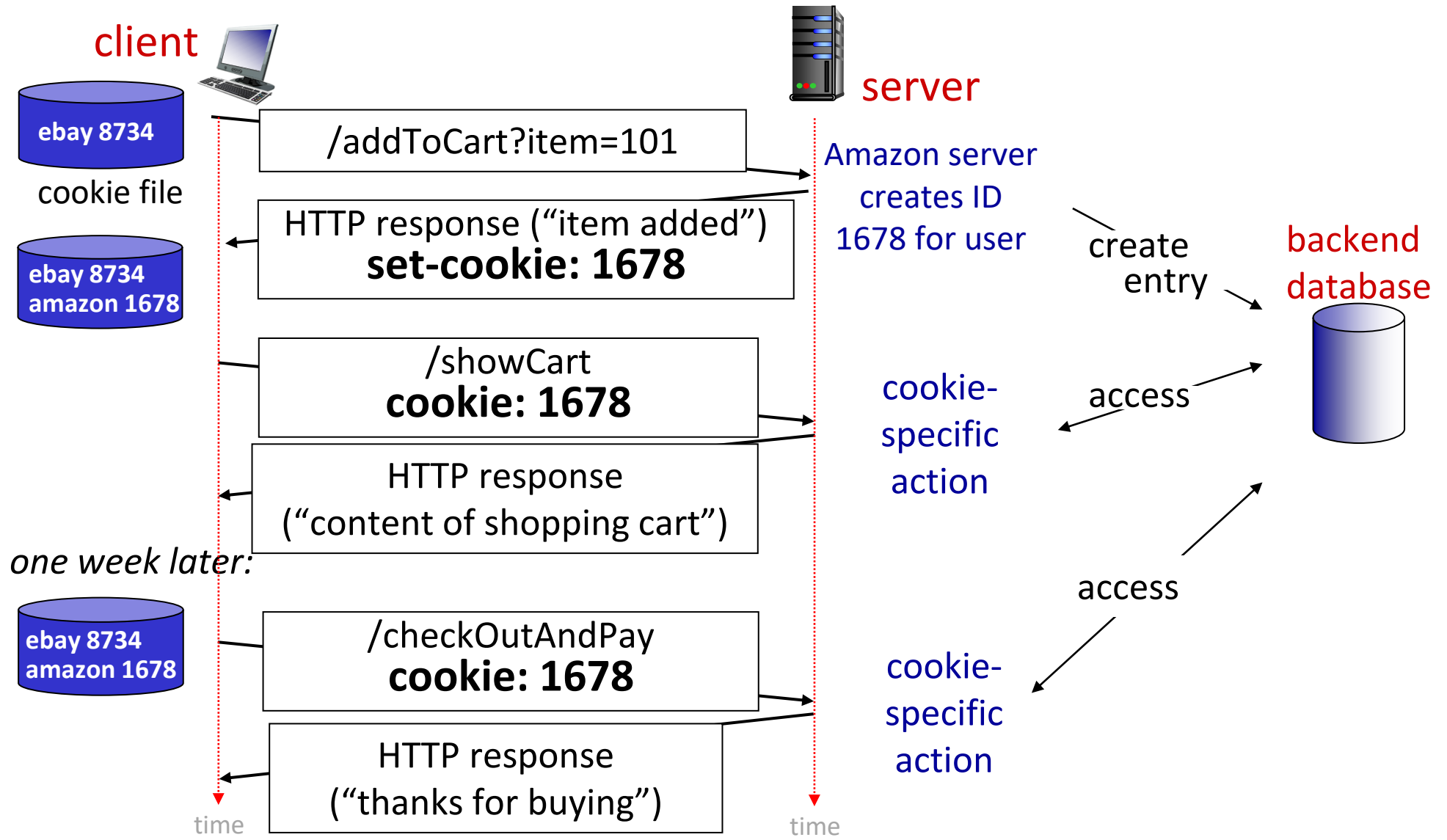
HTTP Response Message



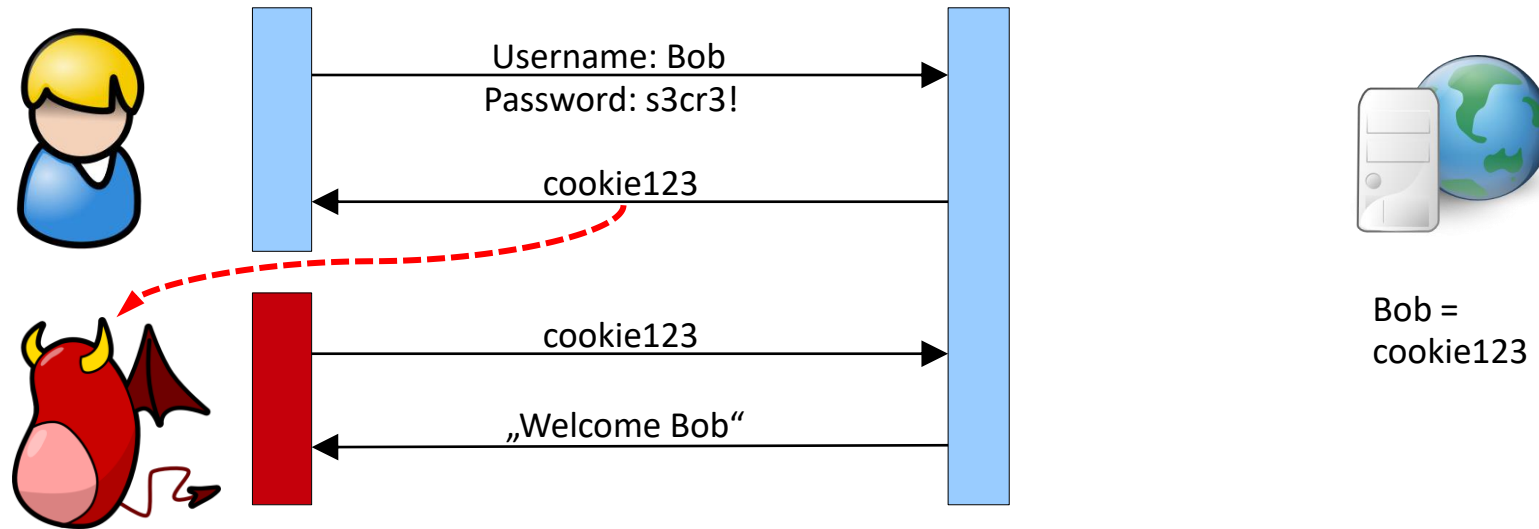
* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

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?



Session Stealing



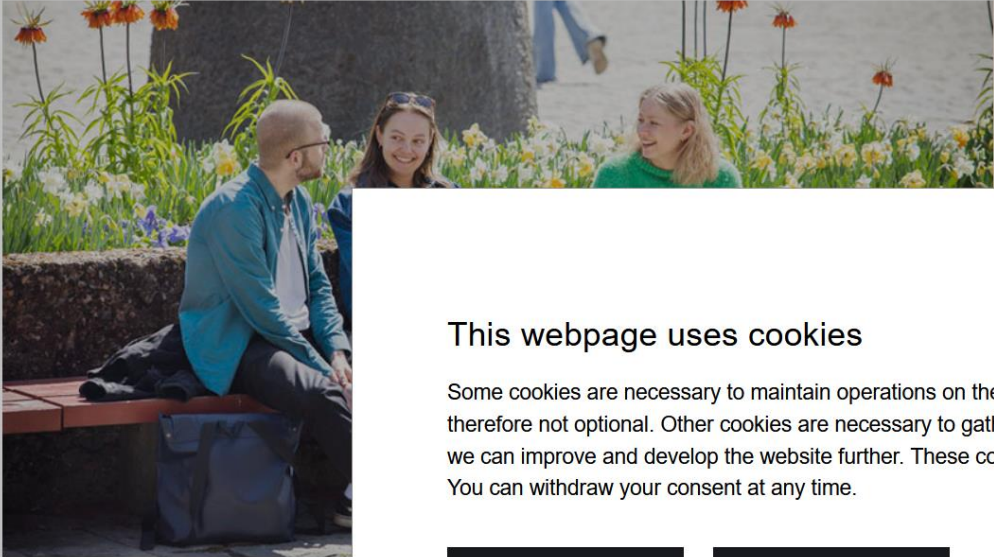
- **Cookie Stealing:**
 - Network eavesdropping (e.g. inside a WIFI or via ARP Spoofing)
 - Redirecting (e.g. DNS Poisoning)
 - Cross-site scripting

UNIVERSITY
OF OSLO

NO

EN

 Menu



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](#)

Norwegian

offers and find the
me that suits you.

ffers

Study

See all study programmes →

Master and phd programmes

→ UiO student? Go to My studies

→ All about studies

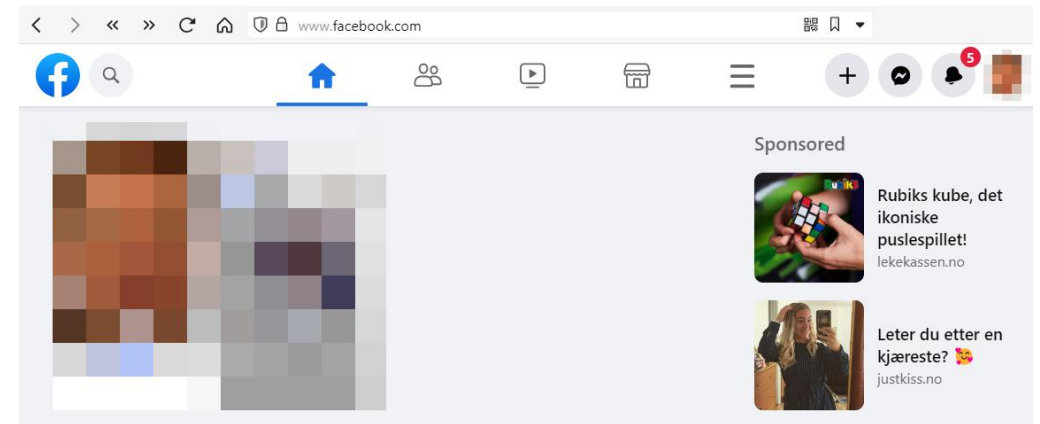
Search in courses

Find schedules, reading lists and exams. [All courses.](#)

→ Canvas

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



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