UPPSALA
UNIVERSITET

Security

Lars-Åke Nordén

UPPSALA UNIVERSITET

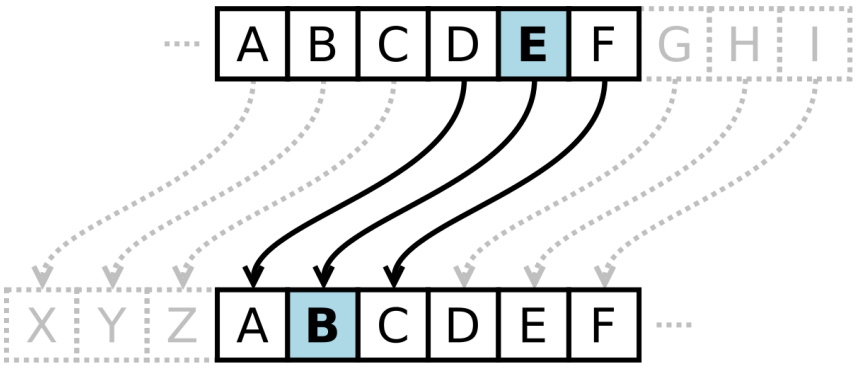
Need for secure communication

- As old as communication through a third party
- Especially in
  - Warfare
  - Diplomacy
  - ...

UPPSALA UNIVERSITET

Classic historical ciphers

Caesar cipher (monoalphabetic)



Vigenere cipher (polyalphabetic)

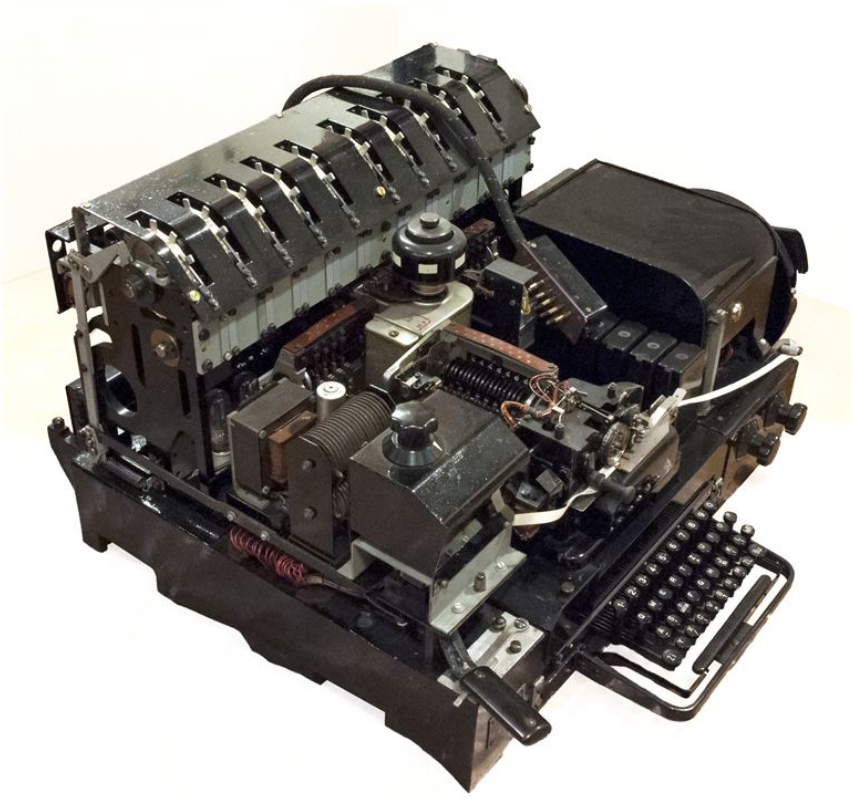
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

UPPSALA
UNIVERSITET

WW cryptosystems

Enigma

Geheimschreiber (T52)



Foundation of modern cryptography

If a lot of smart people for a long time have failed to solve a specific problem, it is unlikely that a solution will appear soon

(hopefully)

UPPSALA UNIVERSITET

Modern cryptography

- Encryption method is well-known
- Secret guarded by a *n-bit key*
  - Encryption and decryption in O(n) time
  - Key guessing in O(2^n) time
- Key management is crucial
- CIA triad represent desirable properties
  - Confidentiality
  - Integrity
  - Availability

UPPSALA UNIVERSITET

Problem: Public key exchange

Alice and Bob wants to communicate. They agree publically on *p* and *g.* After that, they do as follows:

Alice	**Bob**
Create secret key S_A	Create secret key S_B
Compute $T_A=g^{S_A}$ *mod* p	Compute $T_B=g^{S_B}$ *mod* p
Send T_A to Bob	Send T_B to Alice
Compute $K_1=T_B^{S_A}$ *mod* p	Compute $K_2=T_A^{S_B}$ *mod p*

How Alice and Bob now use
K_1 and K_2 to communicate securely?

UPPSALA UNIVERSITET

Solution

- $K_1 == K_2$
  - $T_B^{S_A} = (g^{S_B})^{S_A} = g^{S_B S_A} = g^{S_A S_B} = (g^{S_A})^{S_B} = T_A^{S_B}$ *mod* p

- Alice and Bob can communicate securely using symmetric key cryptography

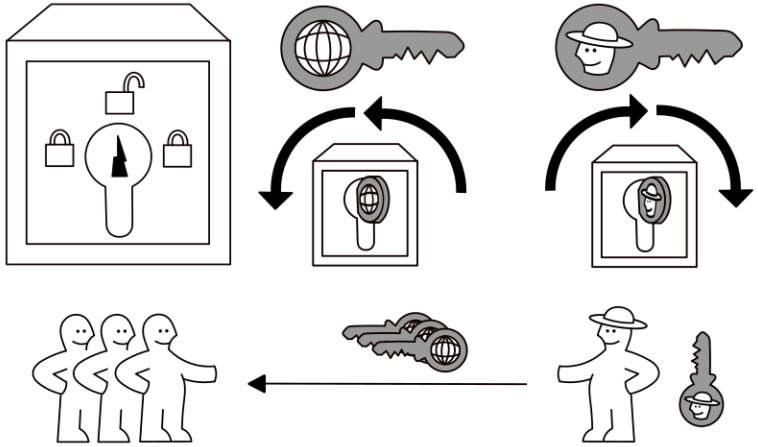
- Method called *Diffie-Hellman key exchange*

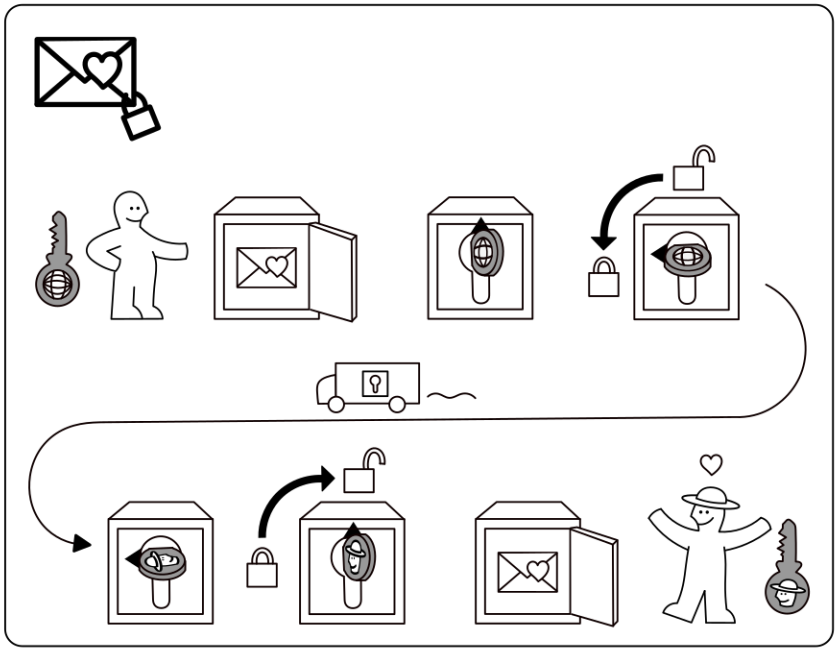
Can Diffie-Hellman be extended to let 3 different users communicate securely?

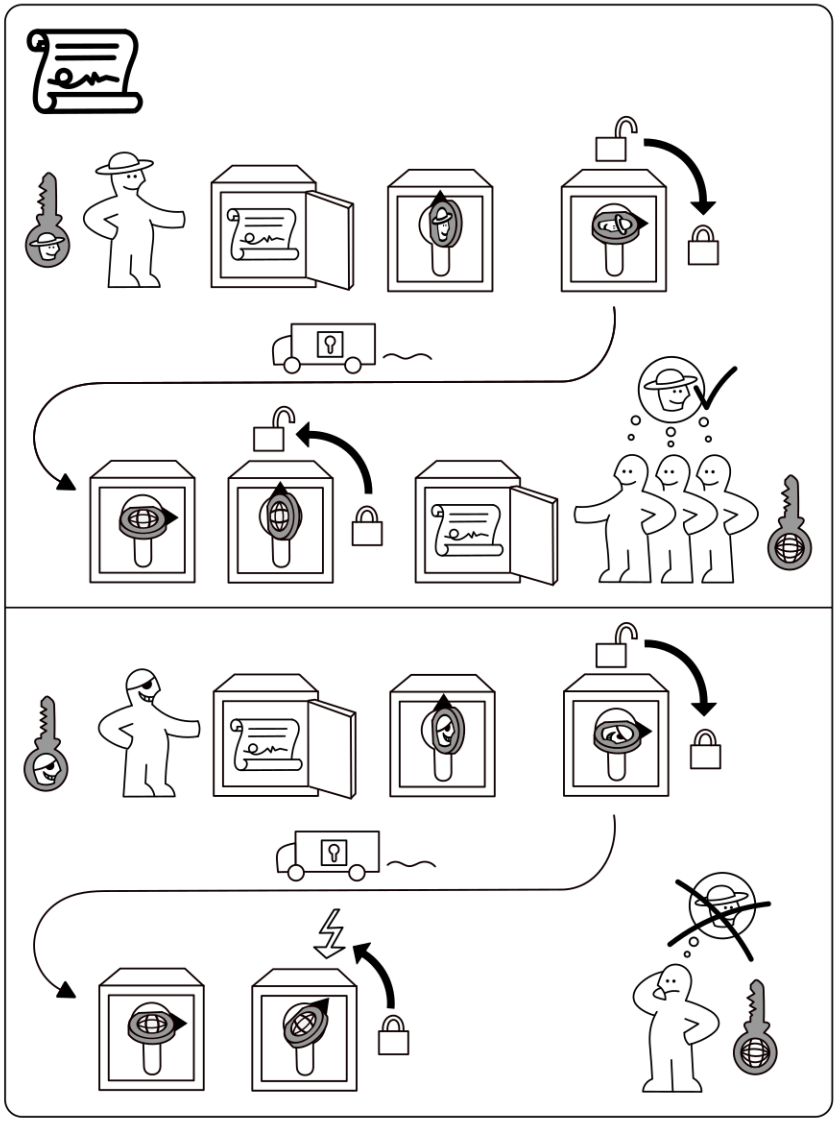
PUBLIK KEY KRYPTO

idea-instructions.com/public-key/
v1.1, CC by-nc-sa 4.0

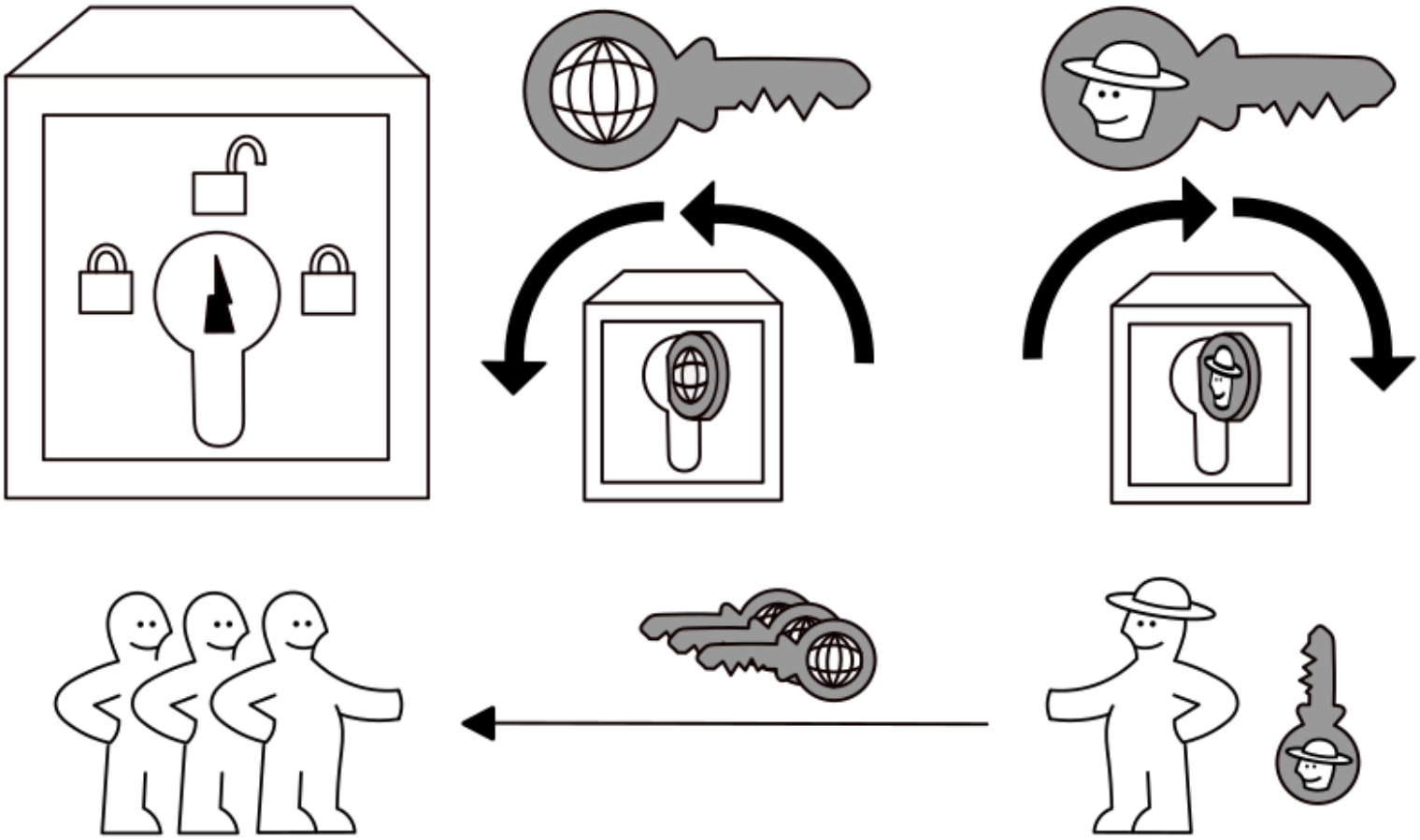
IDEA

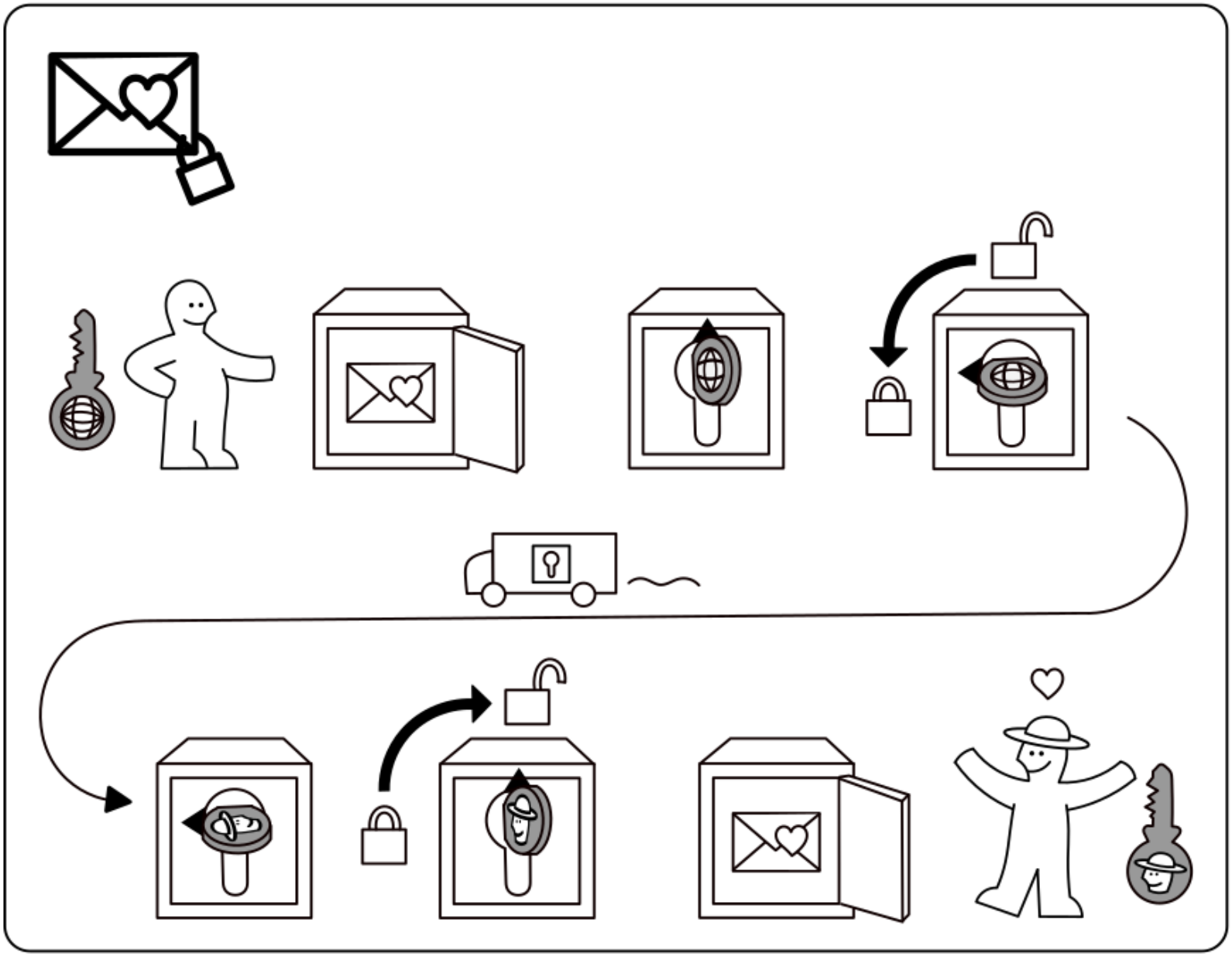


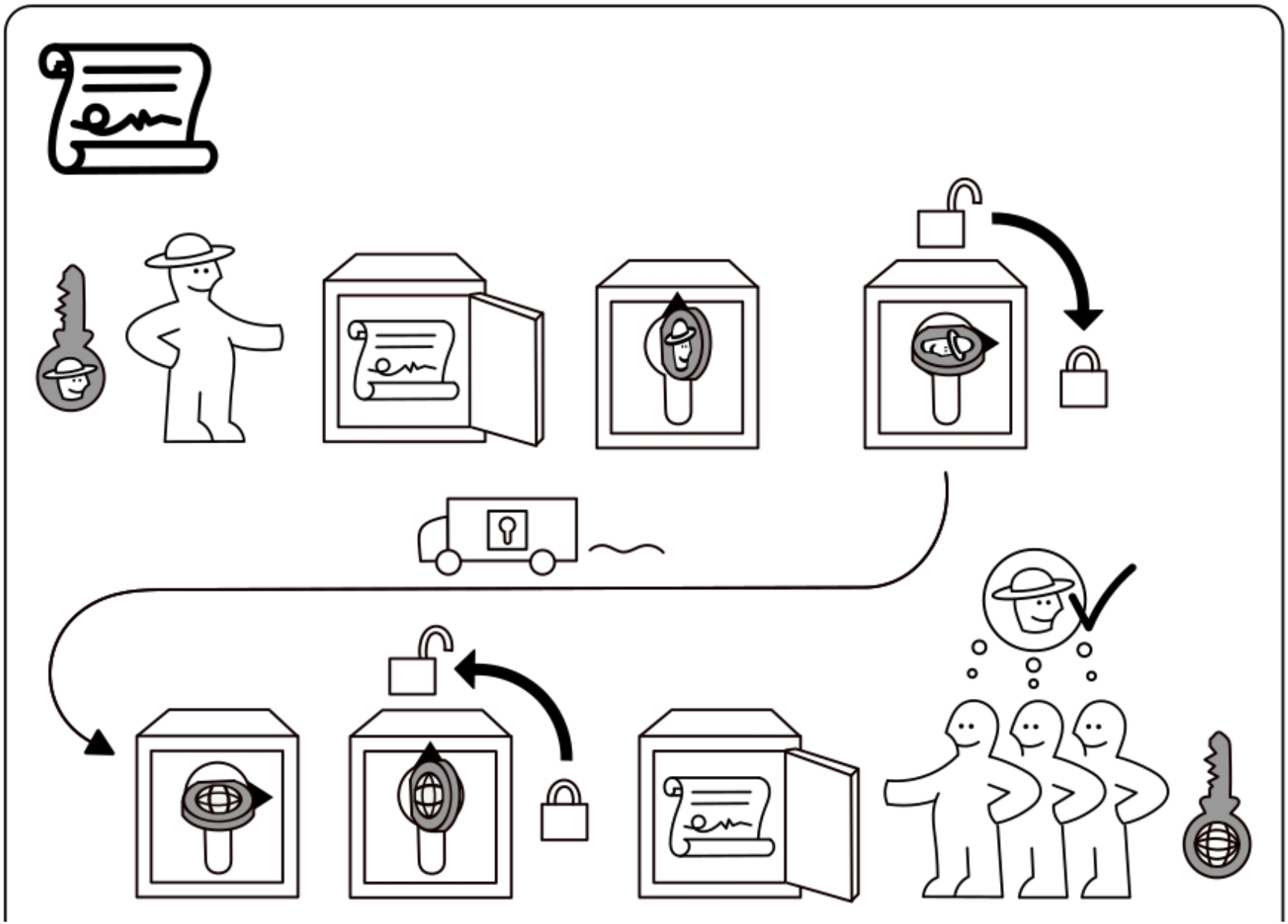


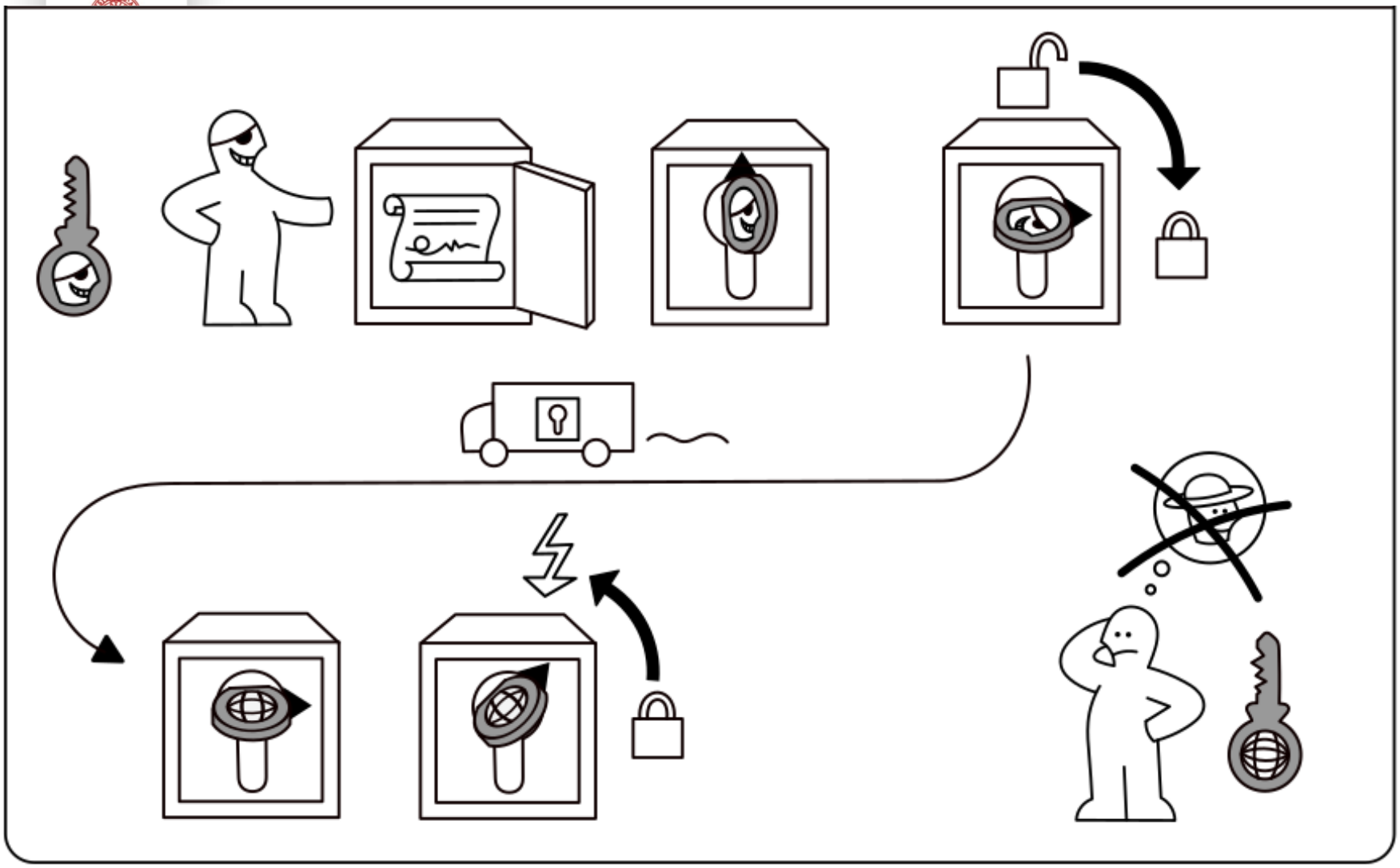


PUBLIK KEY KRYPTO



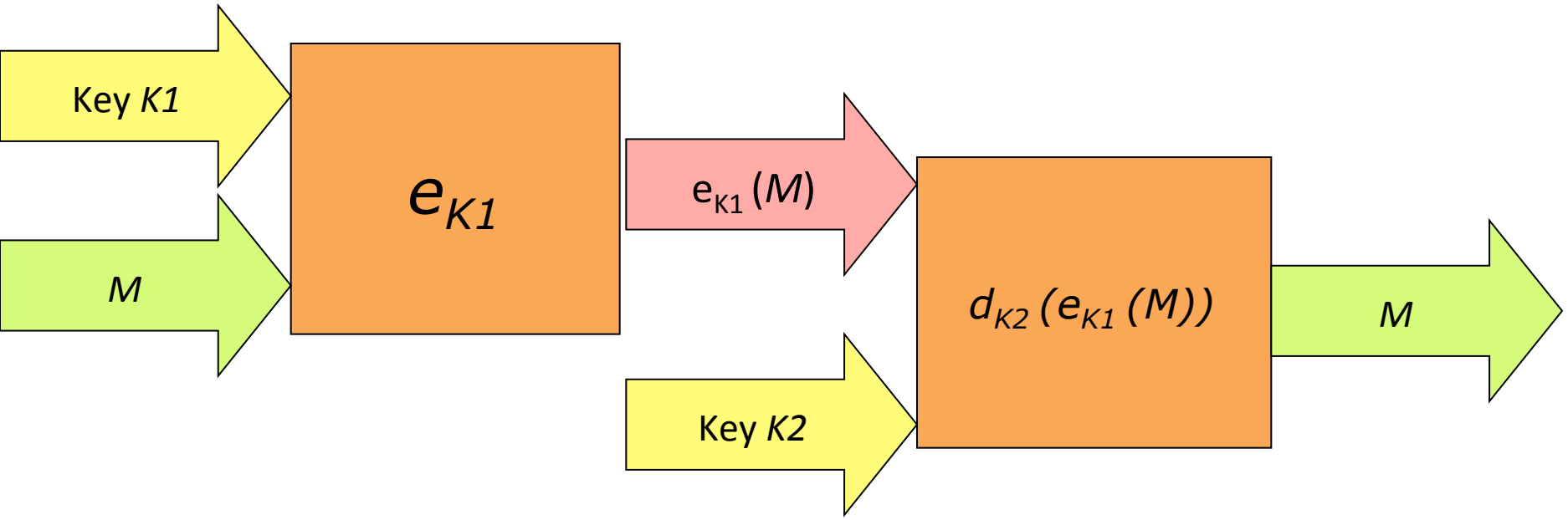






UPPSALA UNIVERSITET

Asymmetric (public-key) encryption



What are pros and cons of this scheme?

UPPSALA UNIVERSITET

Public-key encryption (contd.)

- Key pairs
  - Private key *S*
  - Public key *P*

- $d_S(e_P(M)) = M$ (Encryption)
- $d_P(e_S(M)) = M$ (Signing)
- $d_{P_B}(d_{S_A}(e_{P_A}(e_{S_B}(M)))) = M$ (Both)

Where to find and how to trust public keys?

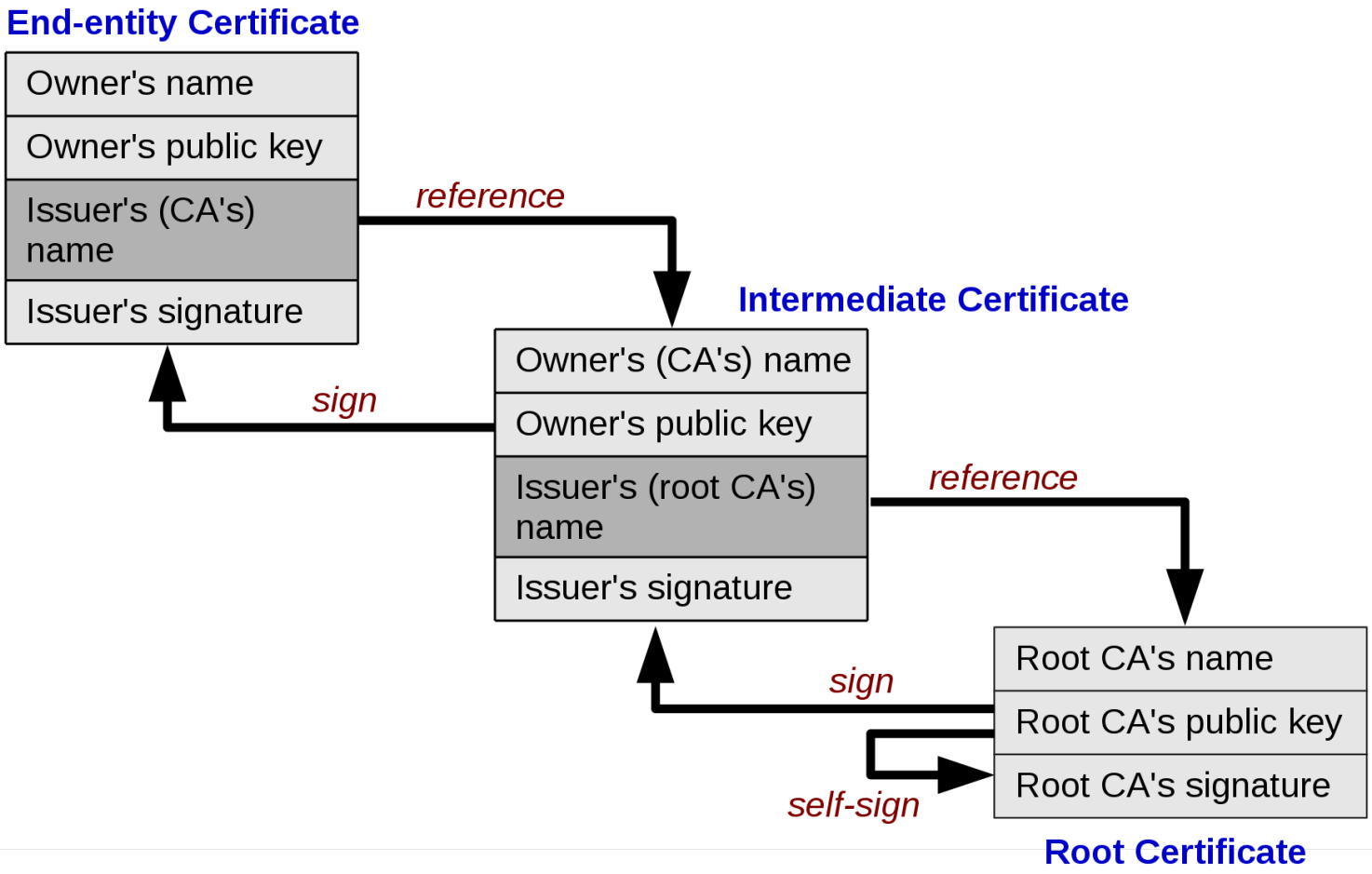
UPPSALA UNIVERSITET

Certification Authority (CA)

- Issues **digital certificates**
  - Digitally signed with the private key of the CA
  - Authorize a public key

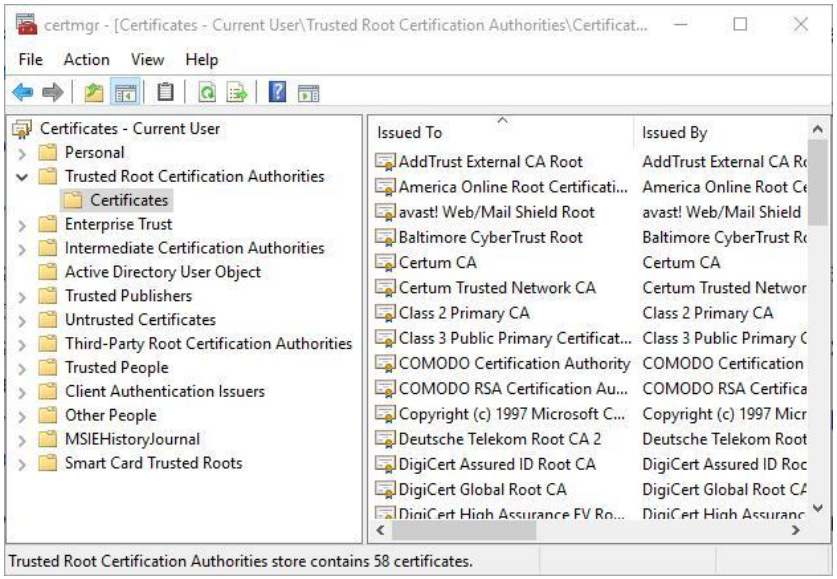
UPPSALA UNIVERSITET

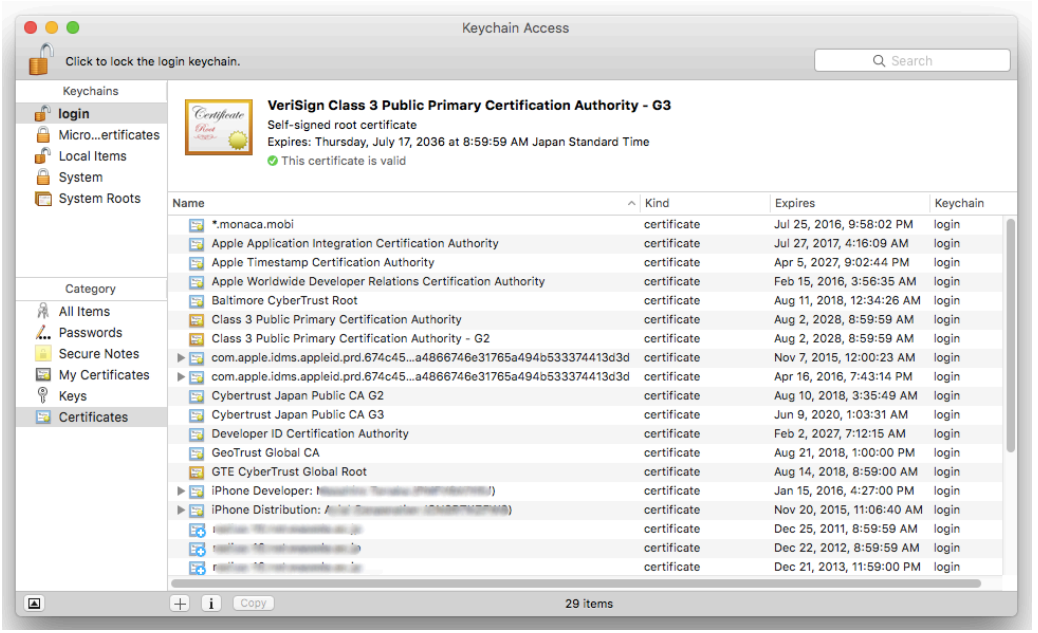
Chain of trust



UPPSALA UNIVERSITET

How to trust the root CA?





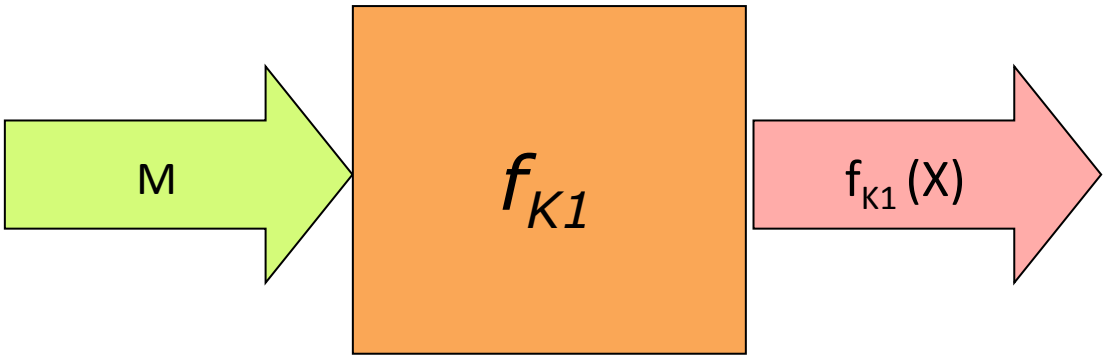
UPPSALA UNIVERSITET

Self-issued certificates

- Some sites present *self-issued* certificates
  - A little lite designing your own drivers license

UPPSALA UNIVERSITET

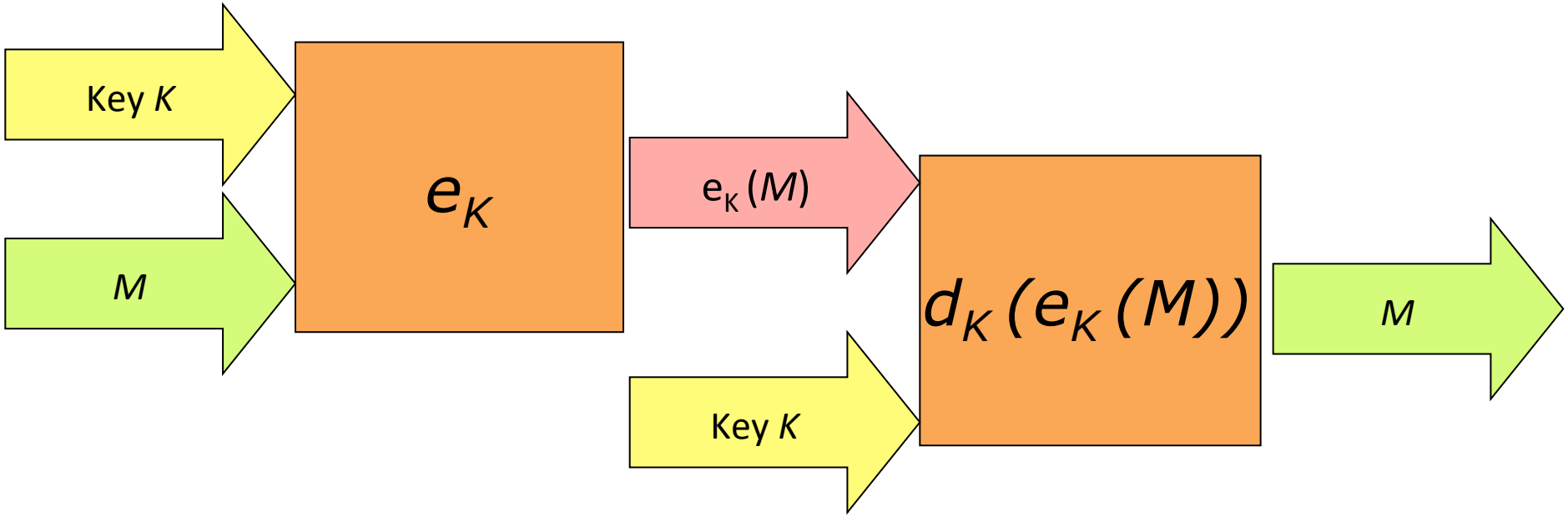
Cryptographic hashing



When is this useful?

UPPSALA UNIVERSITET

Symmetric encryption



What are pros and cons of this scheme?

Usage of modern cryptography

- Symmetric cryptography in encrypted sessions
  - public-key cryptography not fast enough
- Asymmetric cryptography in certain situations
  - To establish a symmetric key
  - Digital signatures and verification
- Cryptographic hashing for verification of authentic data

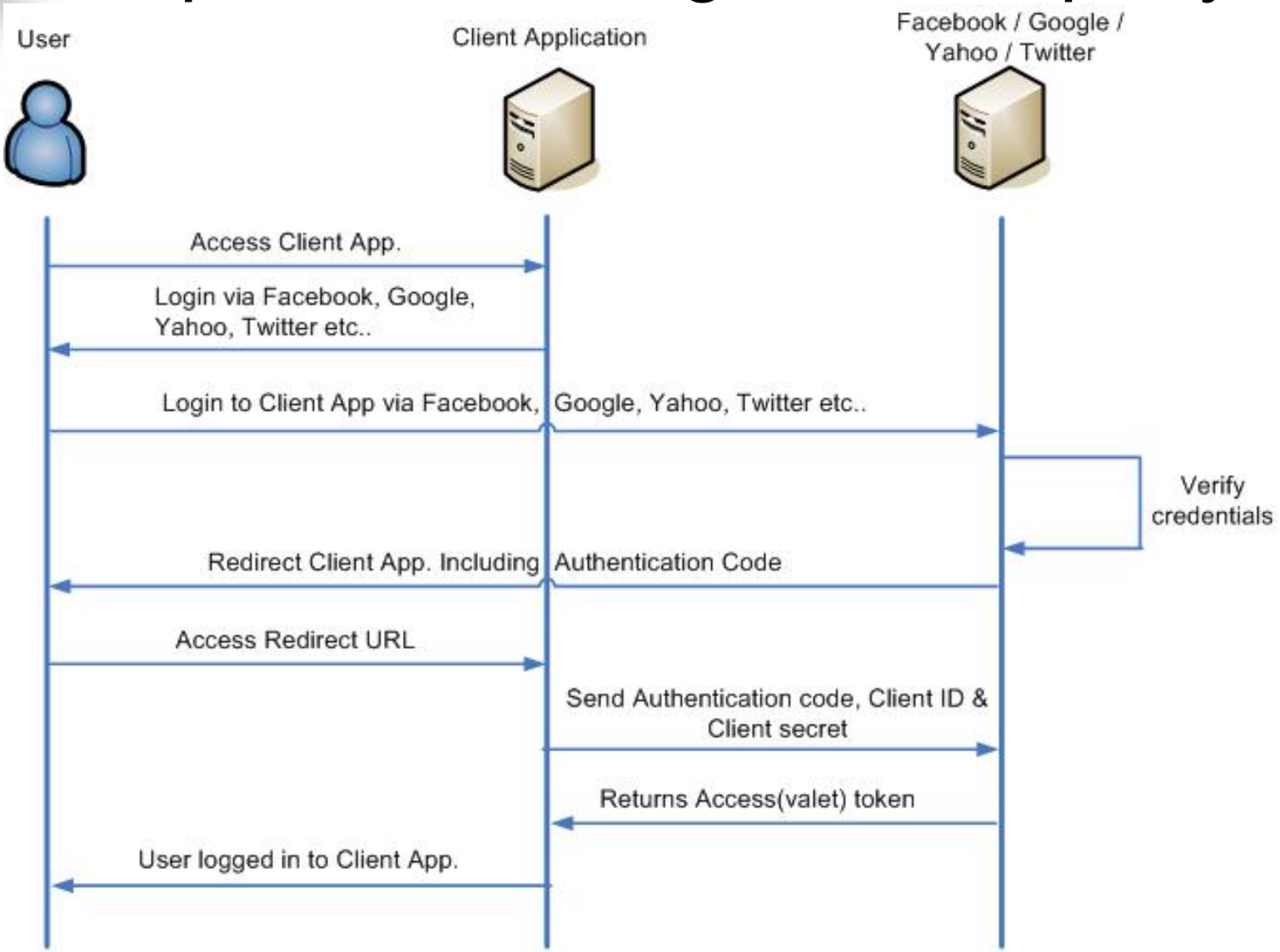
UPPSALA UNIVERSITET

Attacks on cryptosystems

- Known plaintext
- Known ciphertext
- Chosen plaintext
- Man-in-middle
- Denial-of-service
- Side-channel
- Brute-force
- Replay
- ...

UPPSALA UNIVERSITET

OpenAuth through trusted party



Authentication

- Two-factor authentication
  - Something you know
  - Something you have
  - Something you are
- Challenges
  - One-time codes

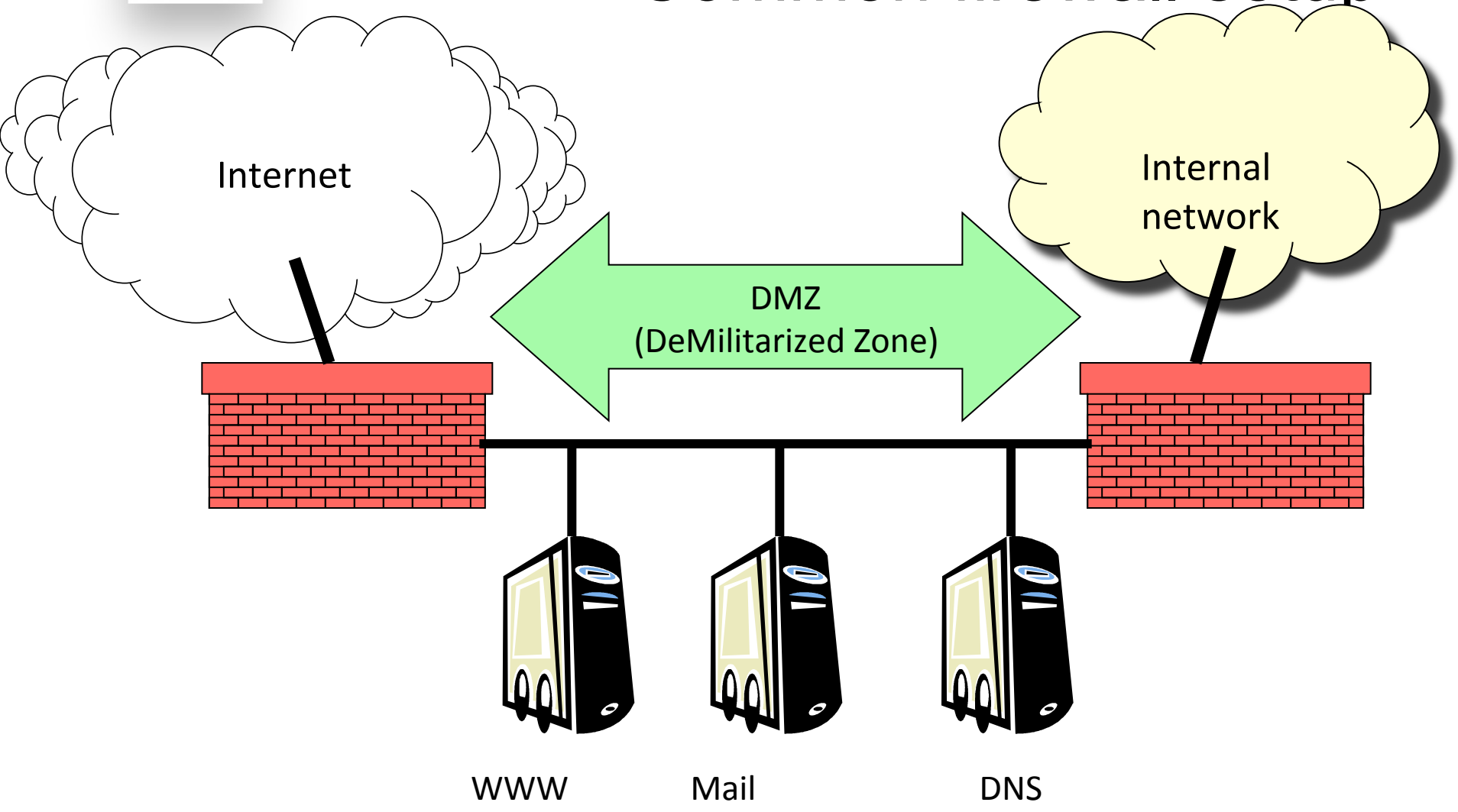
UPPSALA UNIVERSITET

Security in the Internet stack

- Application layer — DNSSEC
- Transport layer — SSL/TLS
- Network layer — IPsec
- Link layer — WEP/WPA
  MAC filtering, ...

UPPSALA UNIVERSITET

Common firewall setup



UPPSALA UNIVERSITET

NAT boxes and security

- Primary goal
  - Avoid over-consumption of global IP addresses
- Side effects
  - Computers with local IP unreachable from outside
  - “Holes” can be opened for servers
  - Servers can be placed in a DMZ
- Often include simple packet filters