ÓBUDA UNIVERSITY, BUDAPEST

SSL CERTIFICATES

Keszthelyi.Andras@kgk.uni-obuda.hu

INTRODUCTION

KESZTHELYI András PhD

Óbuda University,

Keleti Károly Faculty of Economics

Keszthelyi.Andras@kgk.uni-obuda.hu

KELETI KÁROLY
GAZDASÁGI KAR

BASIC RULE

Ask

questions

whenever

you

need!

(Or whenever you think you need:)

Question

- What is the title of this lesson?

STRUCTURE

- **Want to hide your data?**
- One-key encryption
- Two-key encryption
- Certificates
- Known problems

Want to hide your data?

- close your computer
- close the door
- use strong passwords
- … … …
- **encryption**

STRUCTURE

- Want to hide your data?
- **One-key encryption**
- Two-key encryption
- Certificates
- Known problems

One-key encryption

- examples
- security rules
  - key is real random series
  - must be kept in secret
- big question
- need a secure channel for key exchange
- remark: more sophisticated methods exist

One-key encryption, example 1.

- This is the key:
  - A = †
  - B = ◁
  - C = ⌘
  - etc.

One-key encryption, example 1.

- † ⊲ ⌘ † ⊲ ⌘ † ⊲ ⌘ † ⊲ ⌘ † ⊲ ⌘ † ⊲ ⌘ † ⊲
- Which is the most frequent sign?
- Letter frequency in the language

One-key encryption, example 2.

- Key: 3 (shift right)
  - A=C
  - B=D
  - C=E
  - etc.
- Which is the most frequent sign?
- Letter frequency in the language

One-key encryption, example 3.

- Key: 34 (shift right)
  - A=C or D
  - B=D or E
  - C=E or F
  - etc.
- This is the plain text

3434 34 343 34343 4343

???? ?? ??? ????? ????

One-key encryption, example 3.

- Key: 34 (shift right)
  - A=C or D
  - B=D or E
  - C=E or F
  - etc.
- This is the plain text

3434 34 343 34343 4343

W

One-key encryption, example 3.

- Key: 34 (shift right)
  - A=C or D
  - B=D or E
  - C=E or F
  - etc.

```
This is the plain text
3434 34 343 34343 4343
W
```

- If you have enough captured text?

One-key encryption, example 3.

- key: the longer the better
- key: the longest the best

Security rules

- key: real random series
- kept in secret
- => 100% secure
- $X + Y = Z$

Question

- Have you ever read a book „800 miles on the Amazon”?
- Have you ever read a book written by Jules Verne?

Big question

- Alice & Bob have their own keys
  - real random series each
  - kept in absolute secret (if exists;)
- Alice encrypts

  Bob also encrypts

  Alice decrypts

  Bob decrypts and reads
- ?

Big question

- Alice & Bob have their own keys
  - KeyA & KeyB
-
  ```
   text + KeyA
  text + KeyA + KeyB
  text + KeyA + KeyB - KeyA =
      = text + KeyB
  text + KeyB - KeyB = text
  ```
- ?

Big question

- Alice & Bob have their own keys
  - KeyA & KeyB
- `msg1: text + KeyA`
  `msg2: text + KeyA + KeyB`
  `postman:` **`msg2 - msg1 = text`**
- So?

Secure channel for key exchange

- if the key must be kept in secret...

...you need a secure channel

- practically: personal meeting
- In the bottom of the copper mine?
- If the other guy lives in New-Zealand?

Remark

- Less or more sophisticated methods do exist

STRUCTURE

- Want to hide your data?
- One-key encryption
- **Two-key encryption**
- Certificates
- Known problems

Tow-key encryption

- secure channel
- theoretical background
  - example: dictionary
  - breakable – Hard enough, so who cares?
  - prime factorization
  - how it works
  - digital signature
- security rules
  - secret (private) key must be kept in secret
  - collected public keys must be checked
- MITM

Secure channel

- for key exchange
- if the other guy lives in New-Zealand
- expensive
- so we'd like to get rid of

Example

- no need for a secure channel for key exchg
- pair of dictionaries

Example

- no need for a secure channel for key exchg
- pair of dictionaries
  - Serbian-English: public key
    place it at Yellow Gulliver
    everyone can use it
  - English-Serbian: secret key
    the only copy is at home
    your dog stands guard
- replace Serbian words of your message

Breakable

- capture an encrypted message
- go to Yellow Gulliver
- search it => You can find the decryption!

Breakable

- ~1.200 pages
- you must carefully read 600 pages approx. to decrypt one word
- 100 word long message: 6.000 pages to read
- So what if it is breakable?

Breakable

- So what if it is breakable?
- Hard enough, so who cares?

Prime factorization

- real method based on

prime factorization

- much-much more secure

Prime factorization

- Try!
- Multiply two 100 digit prime numbers
- Find the factors of the result!

How it works

- for the exact math background see: Wikipedia, e.g.
- pair of keys are generated public (P) and secret (S)
- one encrypts, other decrypts (and vice versa)
- (secret OR private key)

How it works

coding [coding(text,P), S] = text

OR

coding [coding(text,S), P] = text

How it works

coding [coding(text,P), S] = text

OR

coding [coding(text,S), P] = text

SO:

- public key can be distributed
- secret key must be kept in secret

How it works

- Alice wants to send an ecrypted msg to Bob – which key will she use?
- A: her own secret
- B: her own public
- C: Bob's public
- D: Bob's secret

How it works

- Bob received an encrypted msg from Ann – which key will he use?
- A: his own secret
- B: his own public
- C: Ann's public
- D: Ann's secret

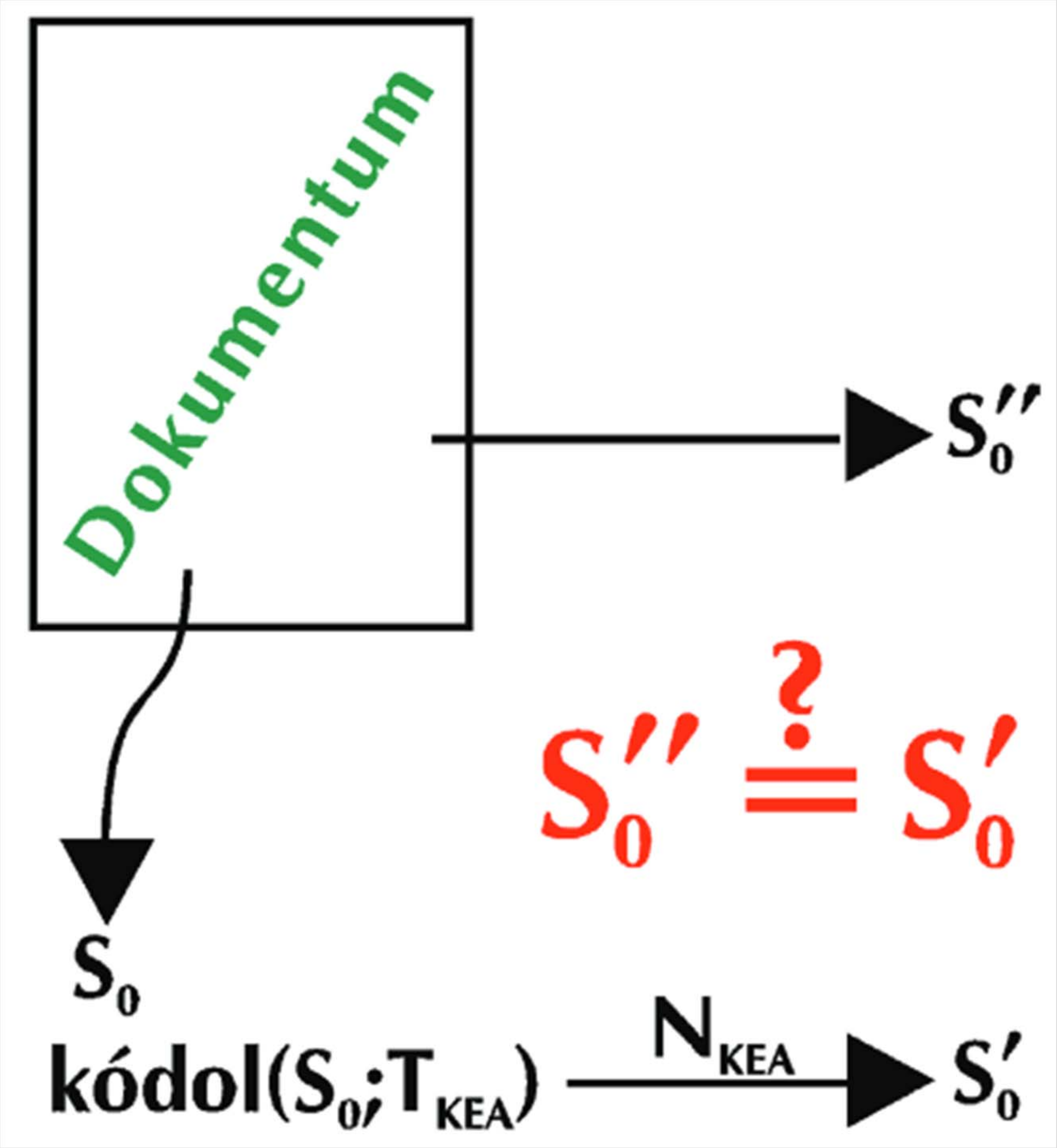
Digital signature

- Ann wants Bob to be sure the message is really from her
- She can encrypt the message with her own secret key, too

Digital signature

- Better solution:
- instead of whole docu you encrypt only a cheksum of the docu

Digital signature


Dokumentum
S_0''
$S_0'' \overset{?}{=} S_0'$
S_0
$\text{kódol}(S_0;T_{KEA}) \xrightarrow{N_{KEA}} S_0'$

Security rule 1.

- **Secret key must be kept in total secret!**
- if not, others may...
  - read our messages
  - digitally sign docus instead of us

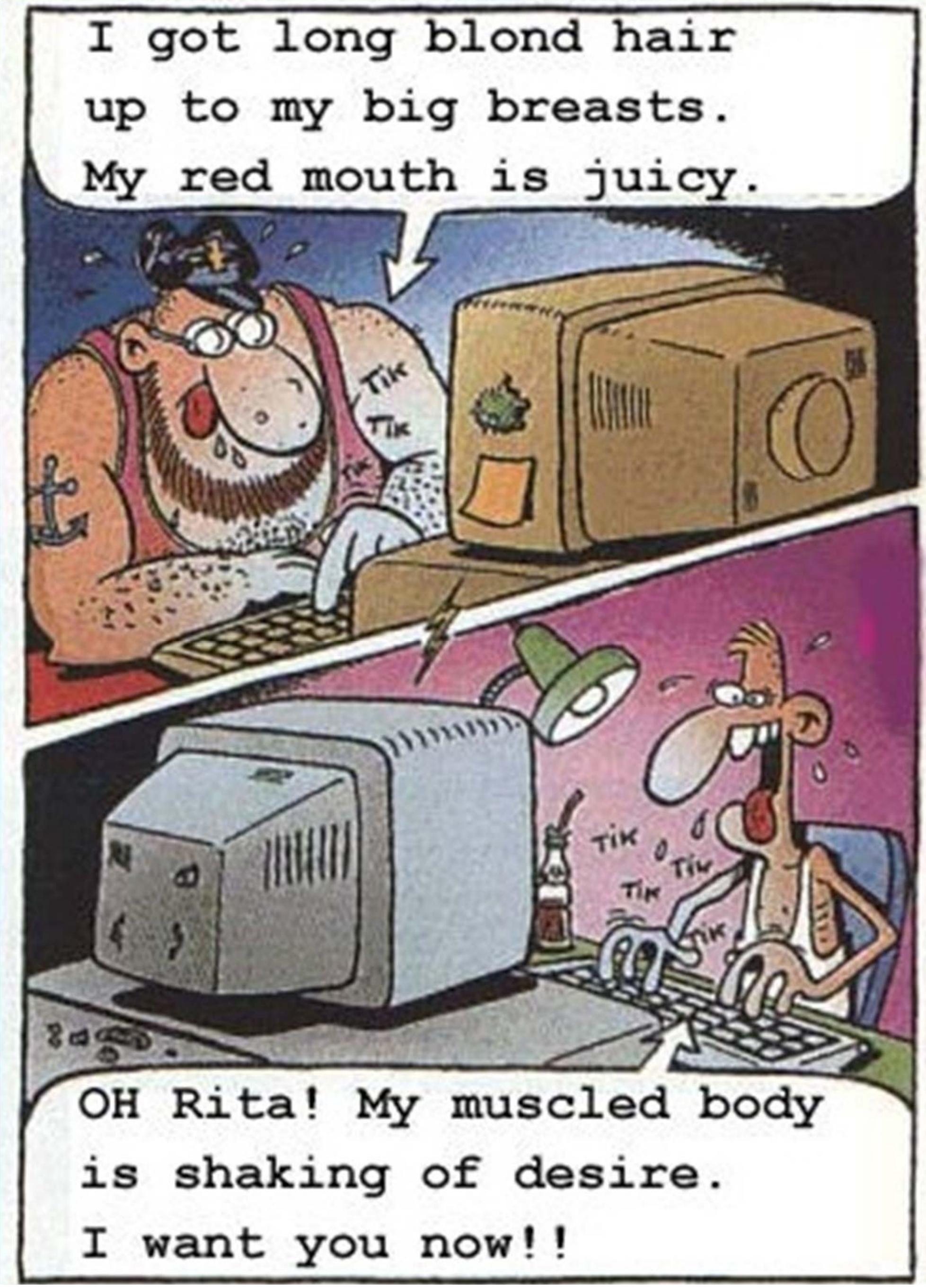
☠ ☠ ☠

Security rule 2.

- **Collected public keys must be checked!**
- Why?

Security rule 2.

- **Collected public keys must be checked!**
- Why?
- For this:


I got long blond hair up to my big breasts. My red mouth is juicy.
TIK
TIK
TIK
TIK
TIK
TIK
TIK
OH Rita! My muscled body is shaking of desire. I want you now!!

MITM

- Man In The Middle
- Monkey In The Middle
- when the other guy is not the one you think he is

MITM

- Alice (P_A;S_A) & Bob (P_B;S_B)
- Alice wants to send

an encrypted msg to Bob

- What does she need for that?

MITM

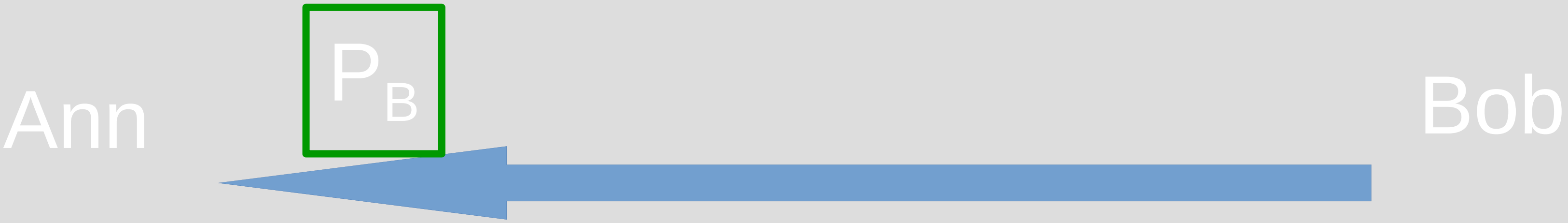
- Alice (P_A;S_A) & Bob (P_B;S_B)
- Alice wants to send

an encrypted msg to Bob

- What does she need for that?
- Bob's public key, P_B.

MITM

- Bob's public key, P_B, can be sent via email



Ann

P_B

Bob

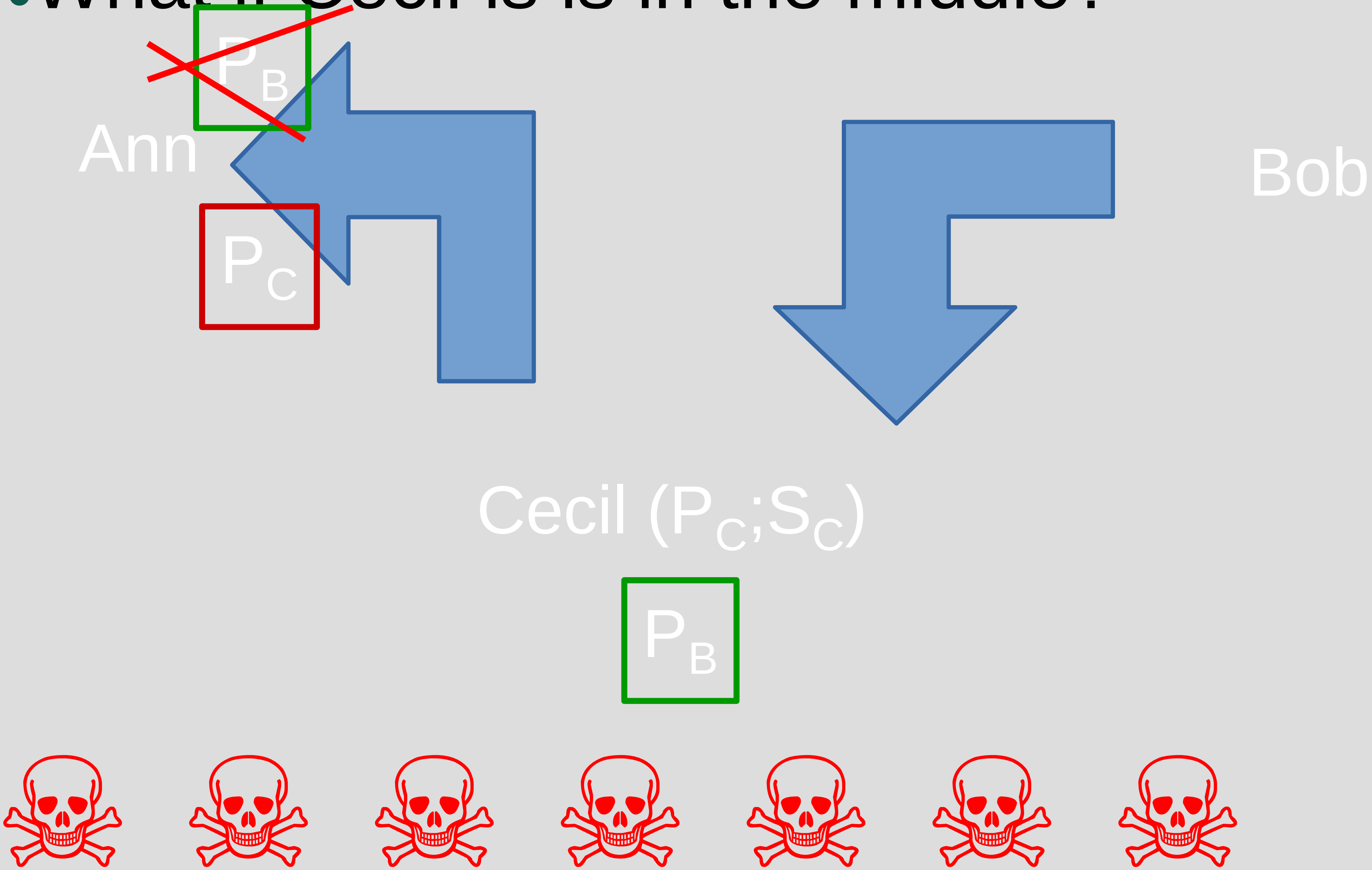
- ...can be?

MITM

- What if Cecil is is in the middle?

MITM

- What if Cecil is is in the middle?



MITM

- You must carefully check
  whether the collected public keys
  really belong to the person
  you think they belong to!

MITM – check public keys

- Get personally from them
- Get via many different channels
- Build the web of trust:

Web of trust

- Alice has the authentic public key of Bob.

Web of trust

- Alice has the authentic public key of Bob.
- Cecil is close to Bob.

Web of trust

- Alice has the authentic public key of Bob.
- Cecil is close to Bob.
- Cecil can put his personal data and his public key into a document.

Web of trust

- Alice has the authentic public key of Bob.
- Cecil is close to Bob.
- Cecil can put his personal data and his public key into a document.
- Bob can sign this document

means: described person

and public key belong to each other.

Web of trust

- Alice has the authentic public key of Bob.
- Cecil is close to Bob.
- Cecil can put his personal data and his public key into a document.
- Bob can sign this document

  means: described person

  and public key belong to each other.
- Alice can check the signature...

Web of trust

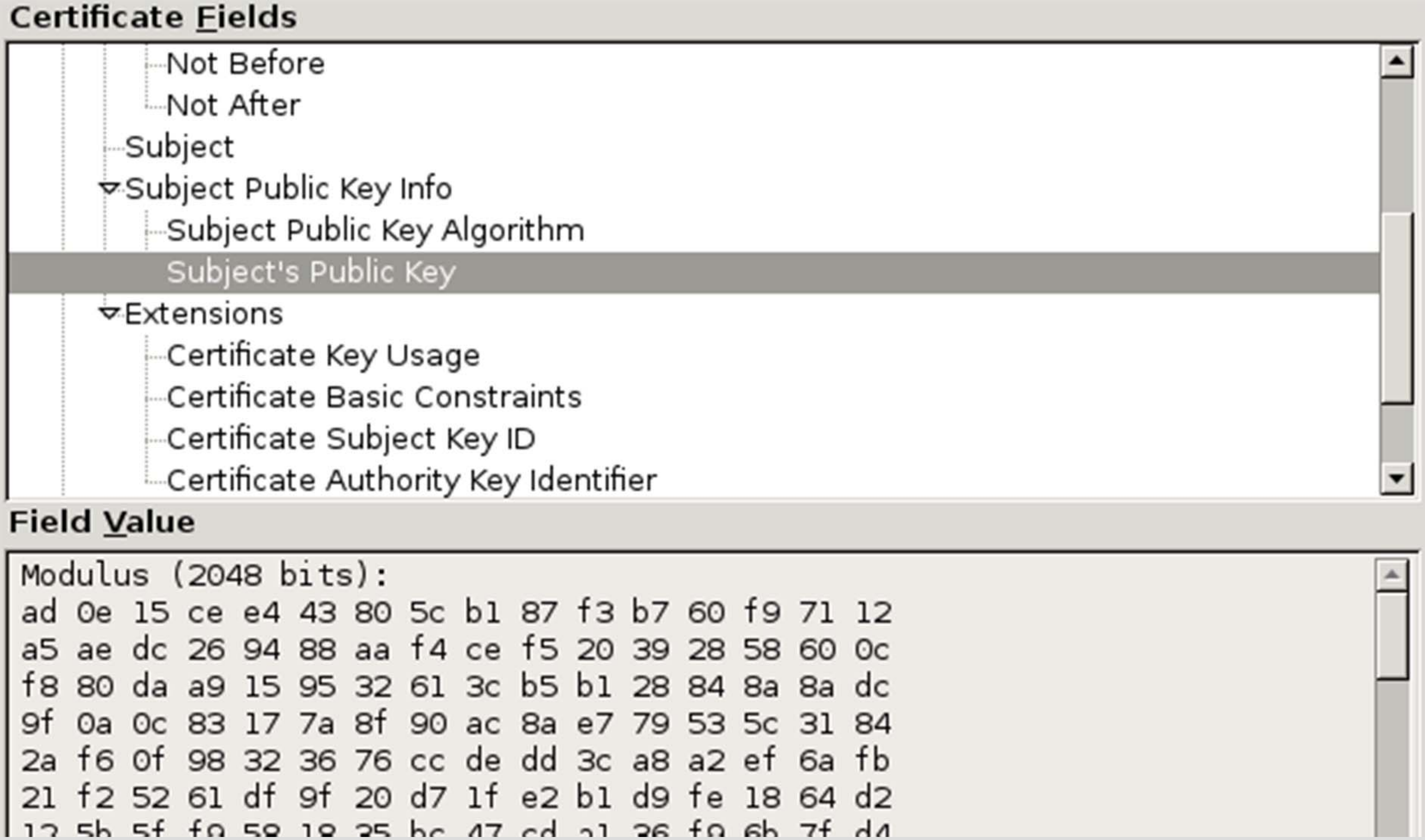
- Chain of trust – web of trust
- No need for central organization

STRUCTURE

- Want to hide your data?
- One-key encryption
- Two-key encryption
- **Certificates**
- Known problems

CERTIFICATES

- standard docu format
for automatic key exchange



```
Not Before
Not After
Subject
Subject Public Key Info
  Subject Public Key Algorithm
  Subject's Public Key
Extensions
  Certificate Key Usage
  Certificate Basic Constraints
  Certificate Subject Key ID
  Certificate Authority Key Identifier
```

```
Modulus (2048 bits):
ad 0e 15 ce e4 43 80 5c b1 87 f3 b7 60 f9 71 12
a5 ae dc 26 94 88 aa f4 ce f5 20 39 28 58 60 0c
f8 80 da a9 15 95 32 61 3c b5 b1 28 84 8a 8a dc
9f 0a 0c 83 17 7a 8f 90 ac 8a e7 79 53 5c 31 84
2a f6 0f 98 32 36 76 cc de dd 3c a8 a2 ef 6a fb
21 f2 52 61 df 9f 20 d7 1f e2 b1 d9 fe 18 64 d2
12 5b 5f f9 58 18 35 bc 47 cd a1 36 f9 6b 7f d4
```

CERTIFICATES

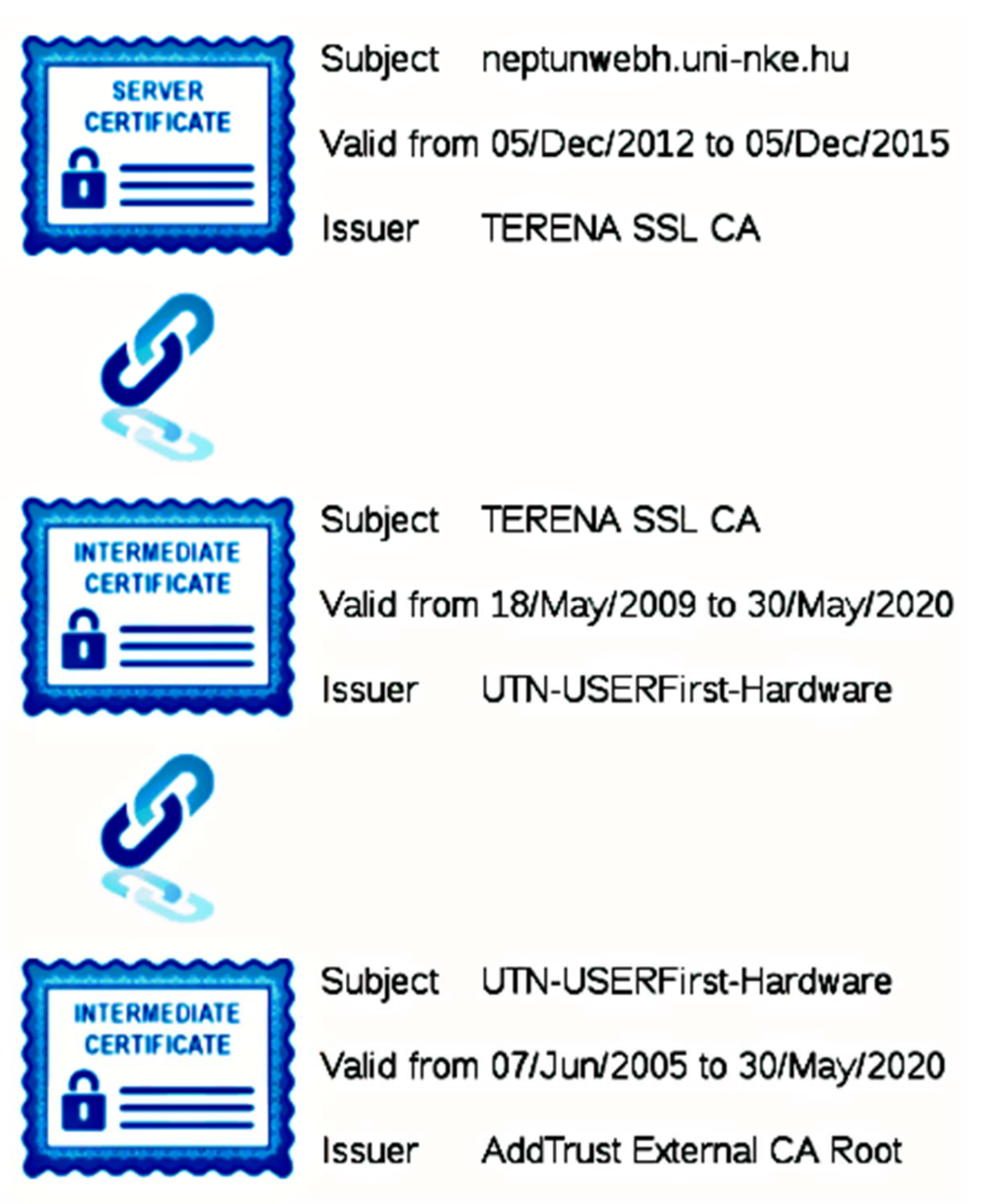
- Certificate Authorities, CA

CERTIFICATES

- See in Firefox, e.g.
- Preferences / Advanced / Certificates
- contains a lot of authentic root CERTs

CERTIFICATES

- in case of an httpS connection:
  - CERT of other side is acquired
  - if it is among the stored ones, OK.
  - if not, its signature is checked
  - (etc.)



Subject neptunwebh.uni-nke.hu

Valid from 05/Dec/2012 to 05/Dec/2015

Issuer TERENA SSL CA

Subject TERENA SSL CA

Valid from 18/May/2009 to 30/May/2020

Issuer UTN-USERFirst-Hardware

Subject UTN-USERFirst-Hardware

Valid from 07/Jun/2005 to 30/May/2020

Issuer AddTrust External CA Root

CERTIFICATES

- if there is an error message,

  it is **YOU**, who must check the situation

  (and the certificate).
- **You must be sure that the other side is the one you think it should be, e.g. your bank!**

STRUCTURE

- Want to hide your data?
- One-key encryption
- Two-key encryption
- Certificates
- **Known problems**

Known problems

- human factor – social engineering
- browser CERTs are tampered with
- a few organizations can probably break it

ADVICES

- Learn what you can – knowledge is power!
- Believe in God AND keep gunpowder dry!
- in other words:
- 100% security level does not exist.
- You want to be as close to it as possible.