Security Fundamentals

DVGC19

KARLSTAD
UNIVERSITY
SWEDEN

Leonardo A. Martucci

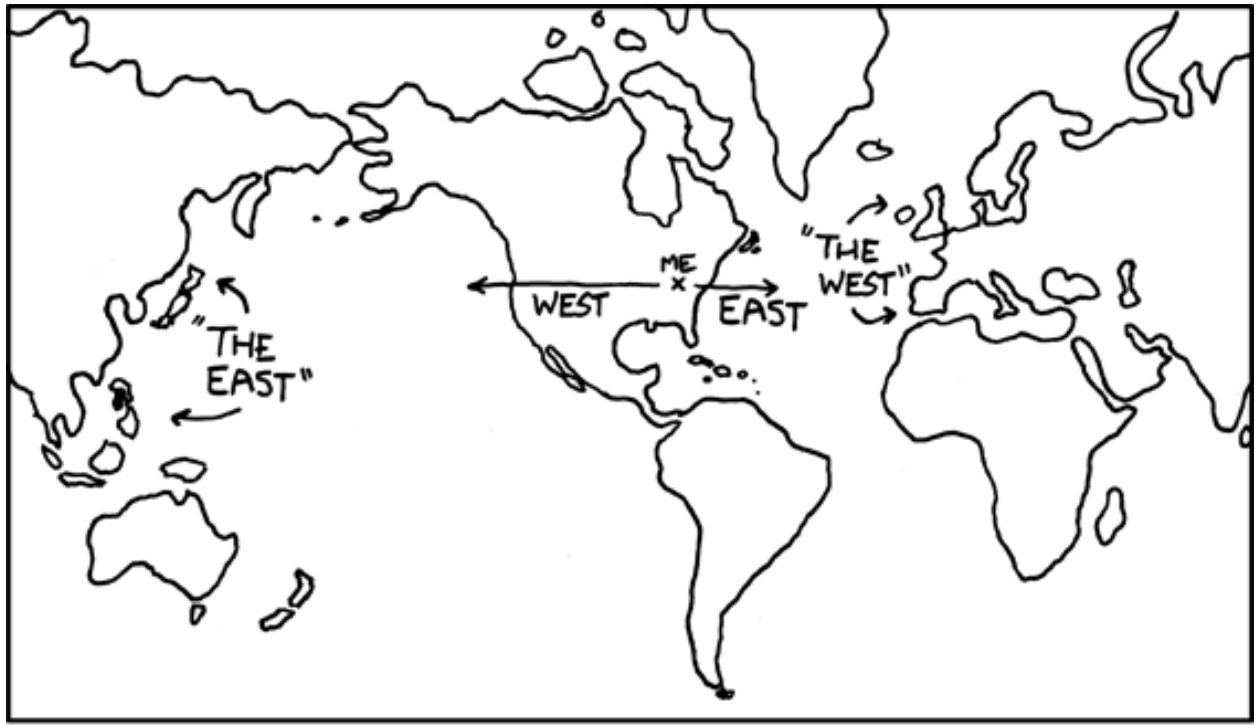
Lectures

1. Introduction to the Course
2. Security Fundamentals (x2)
3. Network Security
4. Firewalls
5. Security at ICA-Gruppen
6. Intrusion Detection
7. Privacy, Security and Ethics
8. Design Principles
9. Web Security
10. Risk Analysis
11. Software Security (x2)
12. Pen Testing

Assignment 1

Assignment 2

Terminology



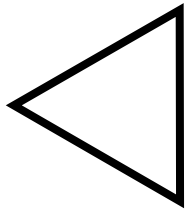
https://www.xkcd.com/503/

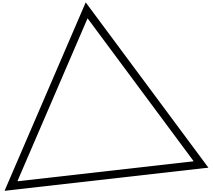
https://www.xkcd.com/1269/

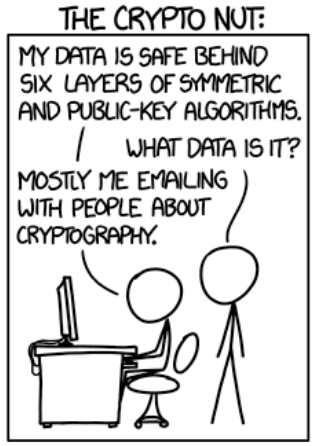
Computer and Network Security

Objectives:

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accounting

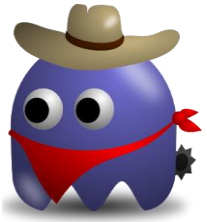




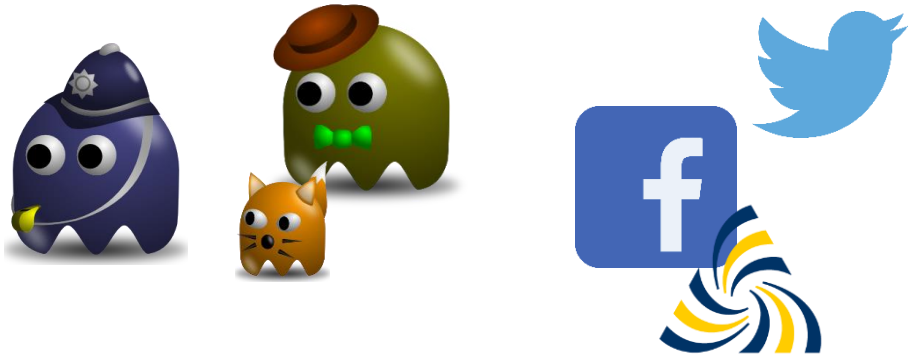


https://www.xkcd.com/1269/

The Actors

- Alice 
- Bob 
- Eve (Mallory) 

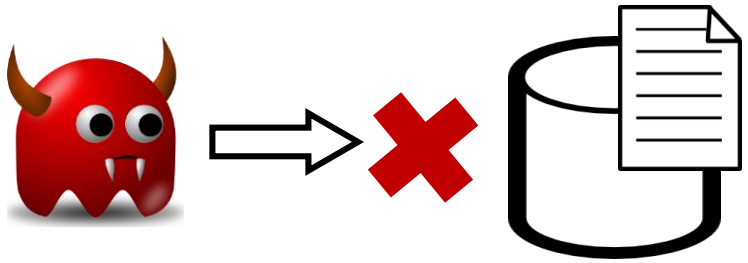
(+ The Support Cast)



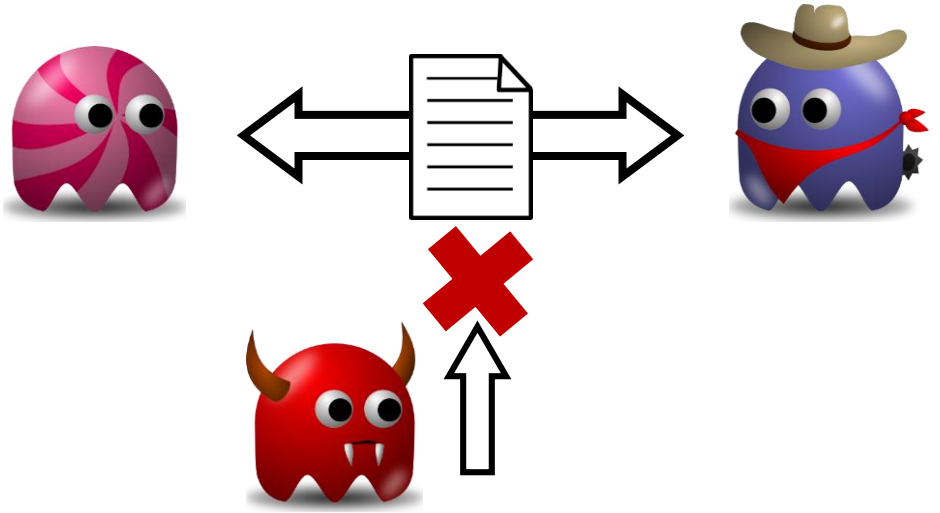
Confidentiality

- Information NOT available or disclosed to unauthorized parties

- Stored Data



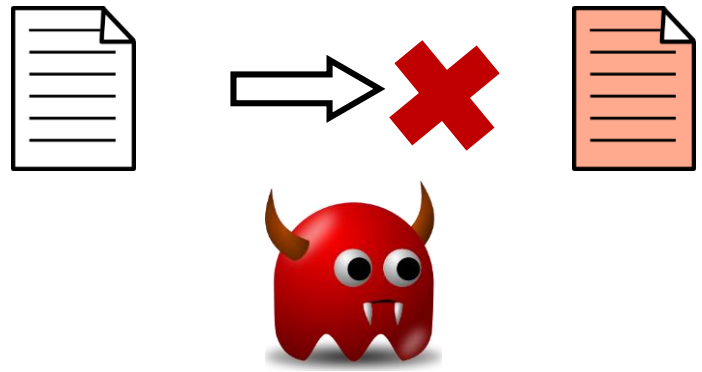
- Data in Transit



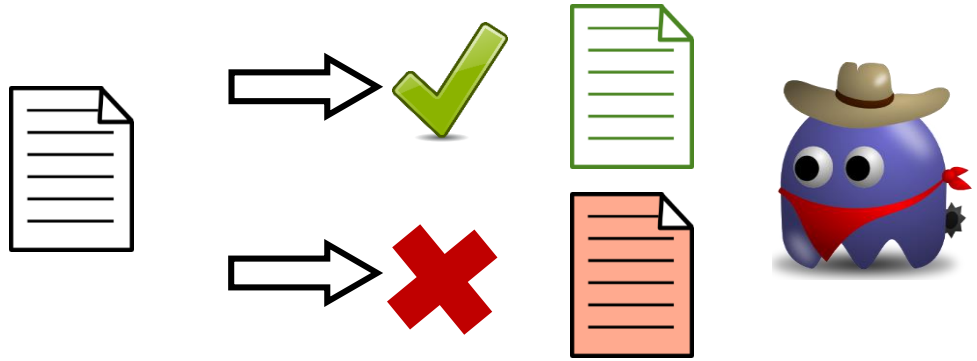
Integrity

- Information NOT modified by unauthorized parties or in an unauthorized manner

- Unauthorized Parties



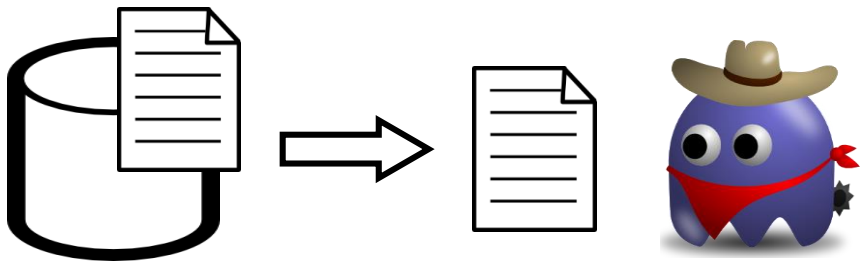
- Unauthorized Manner



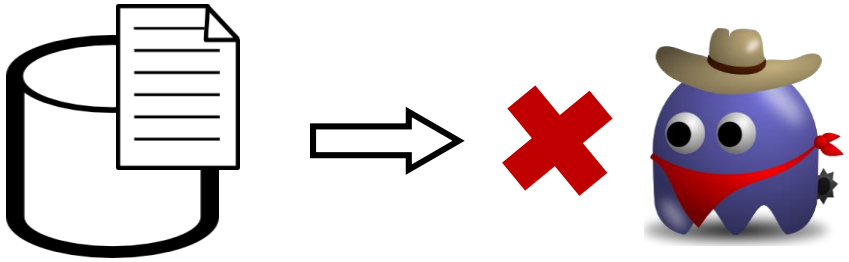
Availability

- Information available when needed

- Available



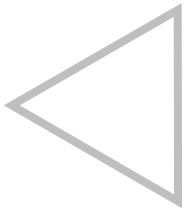
- NOT Available



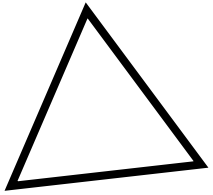
Computer and Network Security

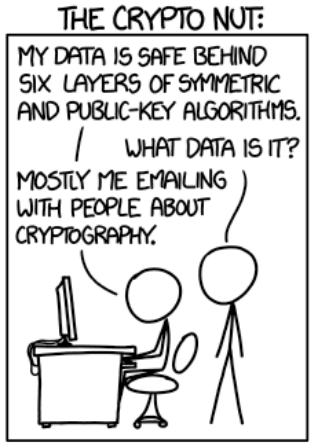
Objectives:

- Confidentiality
- Integrity
- Availability



- Authentication
- Authorization
- Accounting





https://www.xkcd.com/1269/

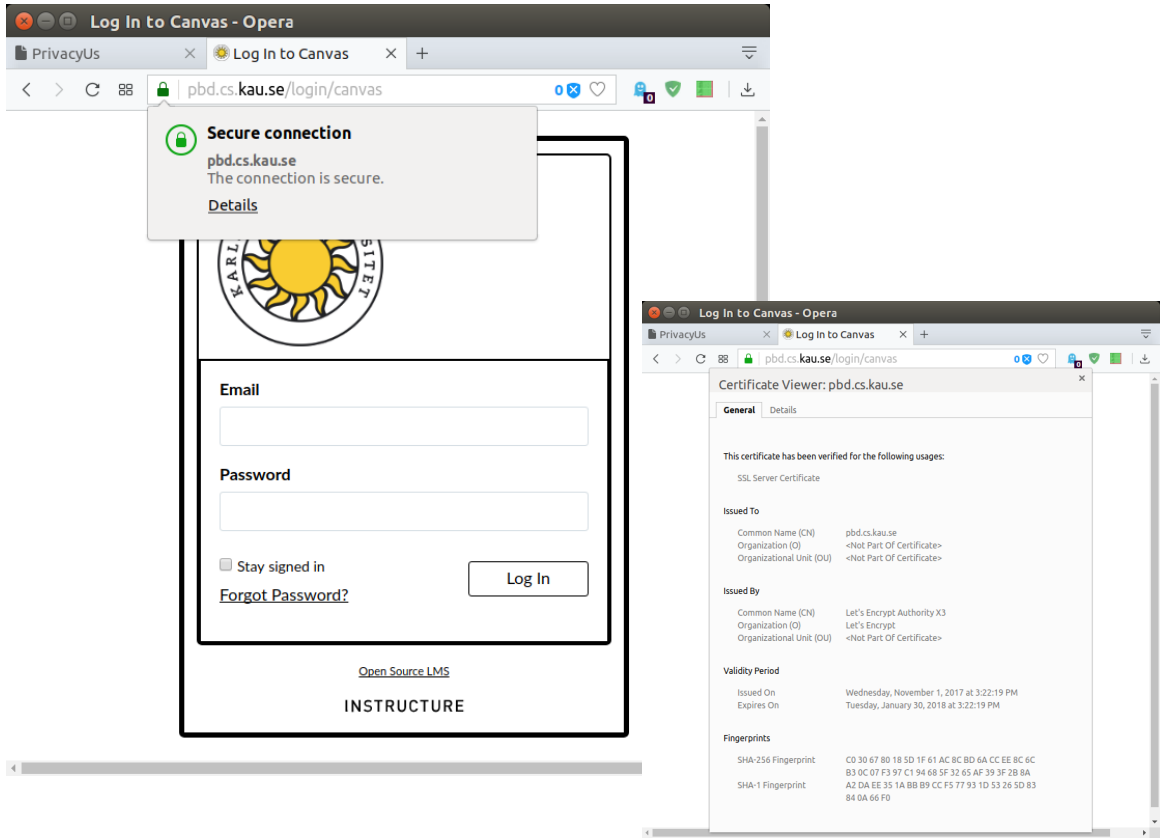
Authentication

- Assurance of an identity claim

Are you really who you claim to be?

- ID cards

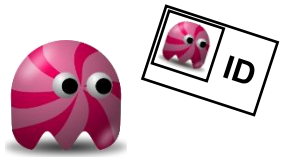
- Digital certificates



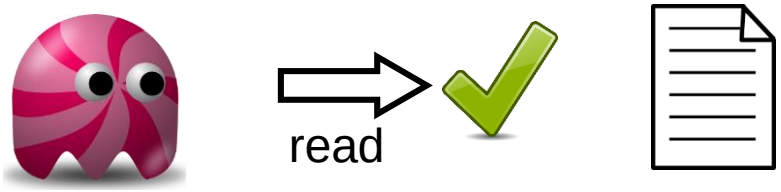
Authorization

- Grant or deny access to resources
  operations over resources

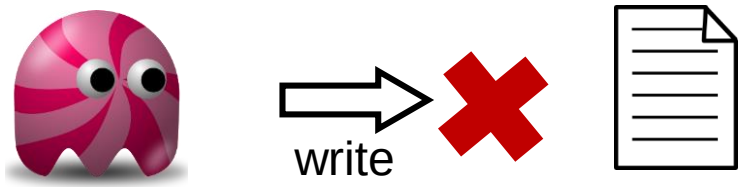
(once authenticated)



- Authorized



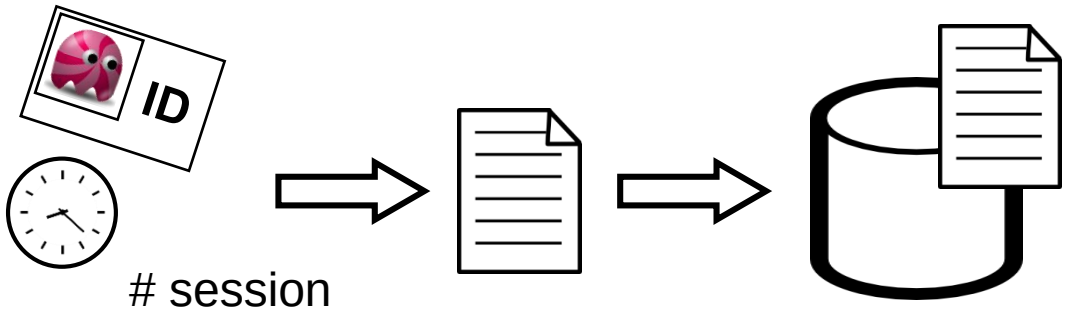
- NOT Authorized



Accounting

- Keeping track of information
  users and data

- Building and storing log data



Cryptomagic

Building Blocks

- message 
- cyphertext 

- encryption function ⇨ e ( )
- decryption function ⇨ d ( )
- key(s) 

Hash Functions

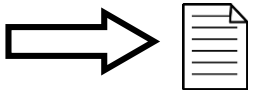
- A one-way function

hash ( ) 

 = message (arbitrary)

 = digest (fixed length)

meaning:

 f () 

+ a number of security properties (C20!)

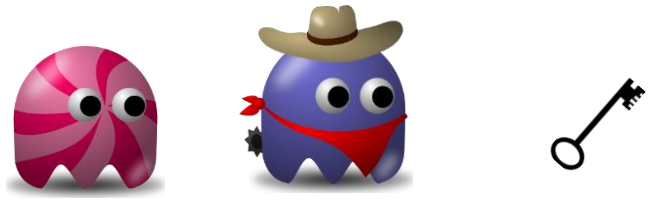
Building Blocks

- message 
- cyphertext 

- encryption function ⇨ e ( )
- decryption function ⇨ d ( )
- key(s) 

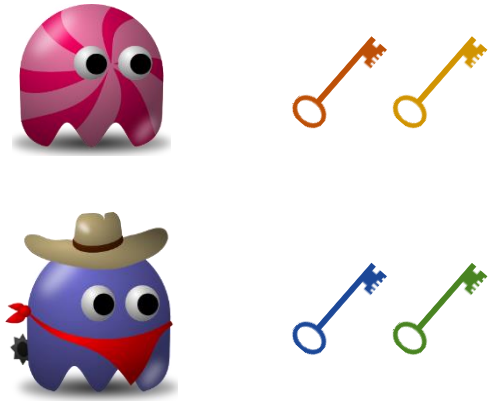
Algorithms and Keys

symmetric



- 1 (shared) key

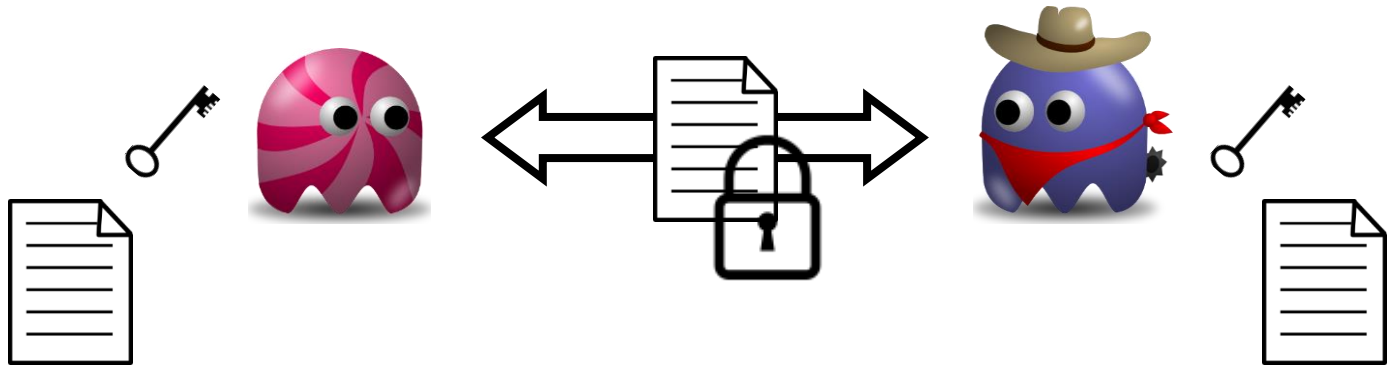
asymmetric

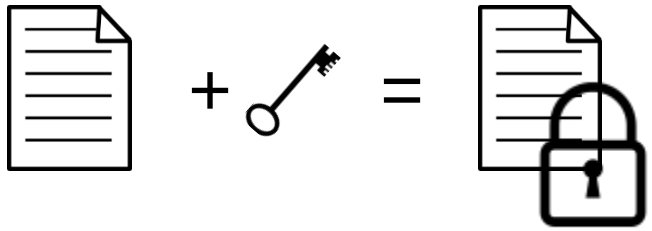


- 2 key pairs

Symmetric Encryption

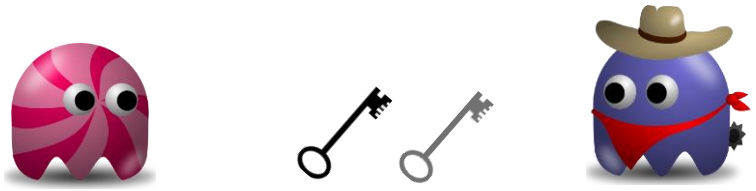
- Alice & Bob → 1 shared key





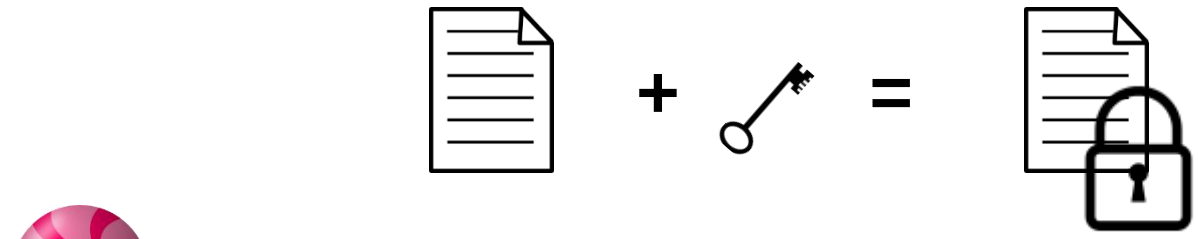
there many ways on how to do (e, d)

Symmetric Encryption in Practice

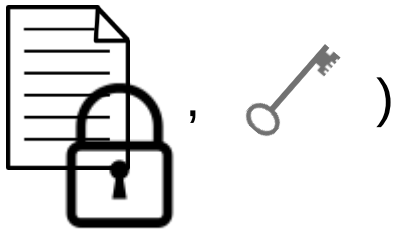


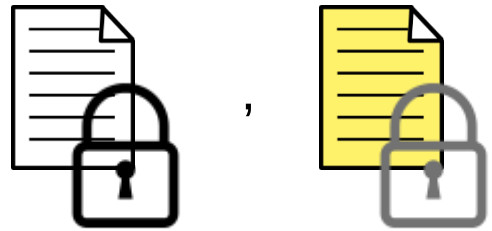
- with symmetric keys:
  authenticated encryption (EtM)

2 shared keys



encrypt-then-MAC message

hash () =

()

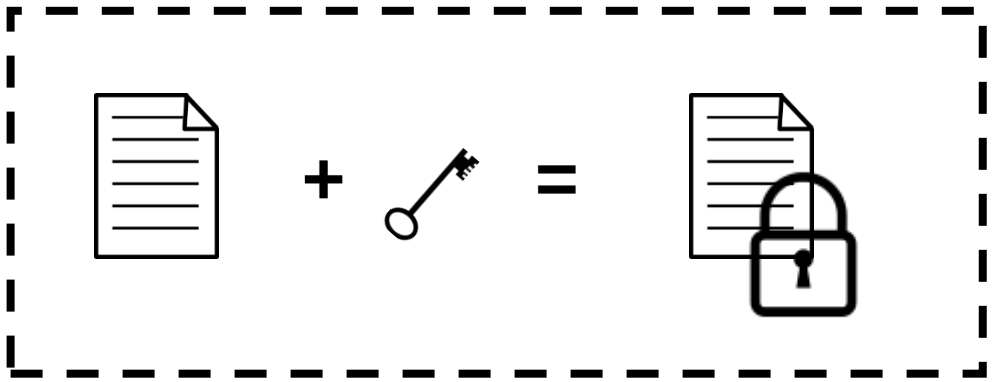
* keyed hash

Symmetric Encryption in Practice

- with symmetric keys:

  authenticated encryption (EtM)

shared key(s)



symmetric encryption

encrypt-then-MAC message

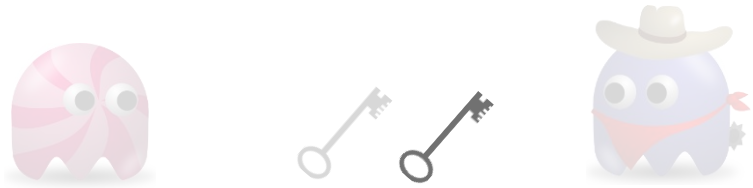
hash (,) =

(,)

* keyed hash

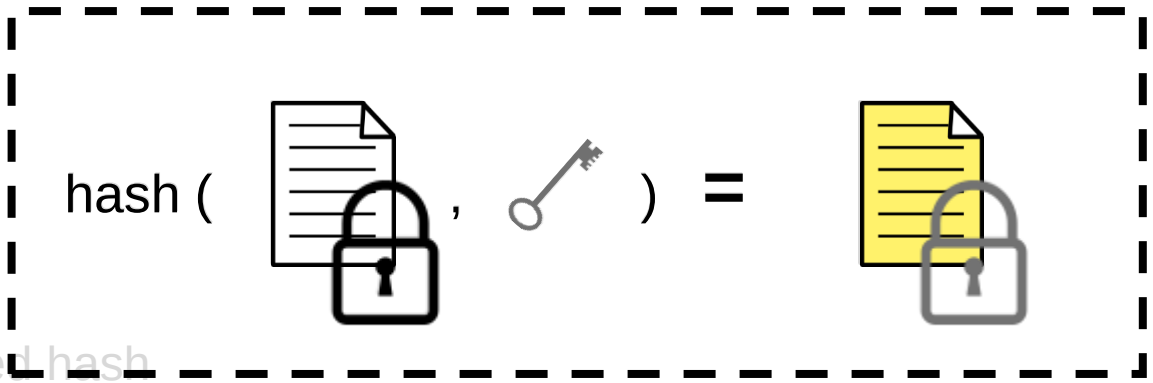
Symmetric Encryption in Practice

- with symmetric keys:
  authenticated encryption (EtM)



shared key(s)

encrypt-then-MAC message



authentication

* keyed hash

Asymmetric Encryption

- Alice & Bob → 2 key pairs

key pair = (public, private)

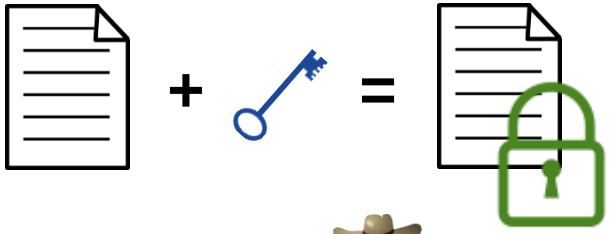
key pair = (public, private)

Asymmetric Encryption: Confidentiality

- For encryption and decryption

key pair = (public, private)

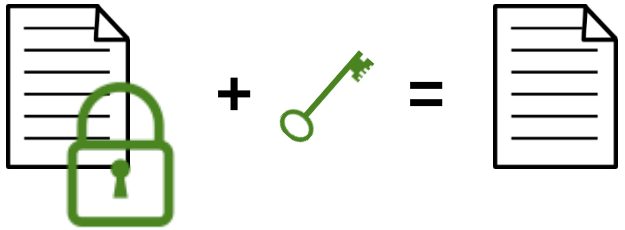
key pair = (public, private)



encrypts with

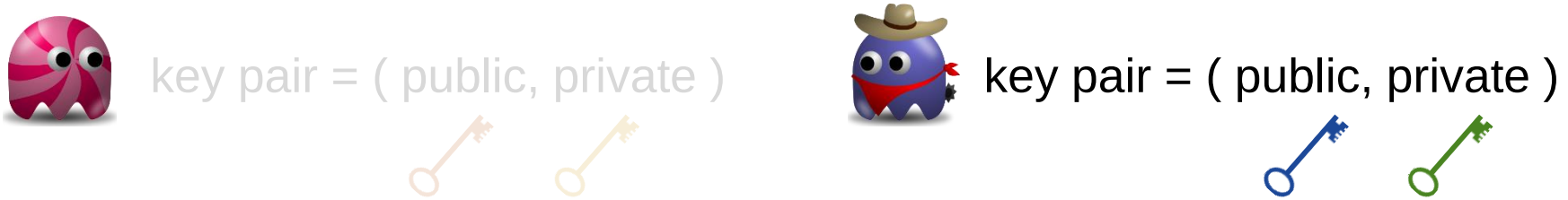
public key

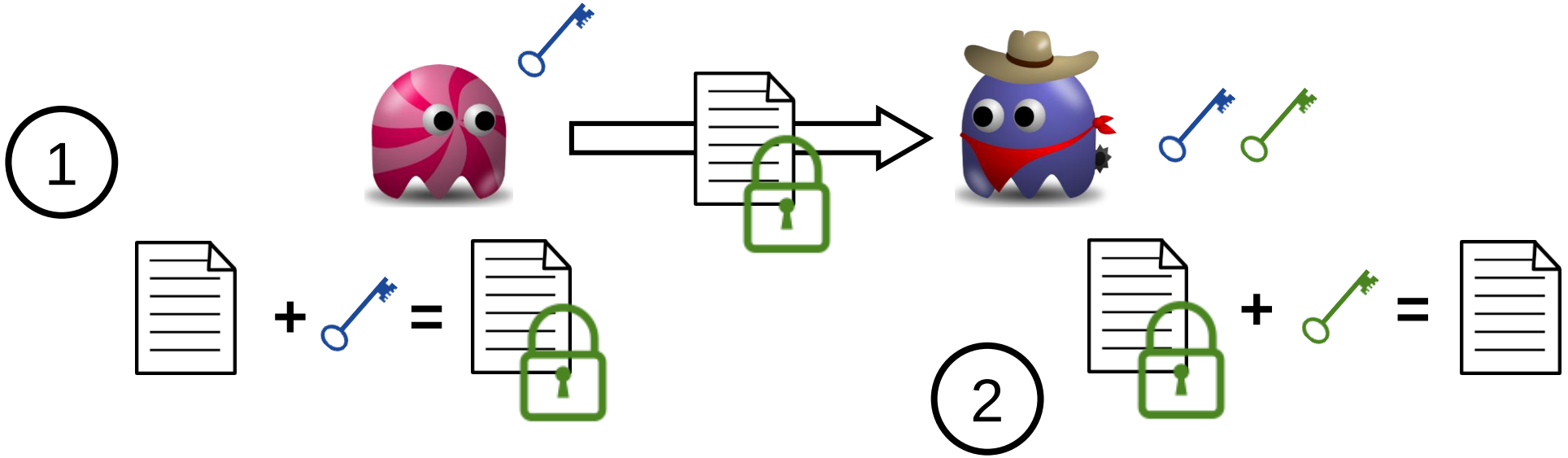
decrypts with his private key



Asymmetric Encryption: Confidentiality

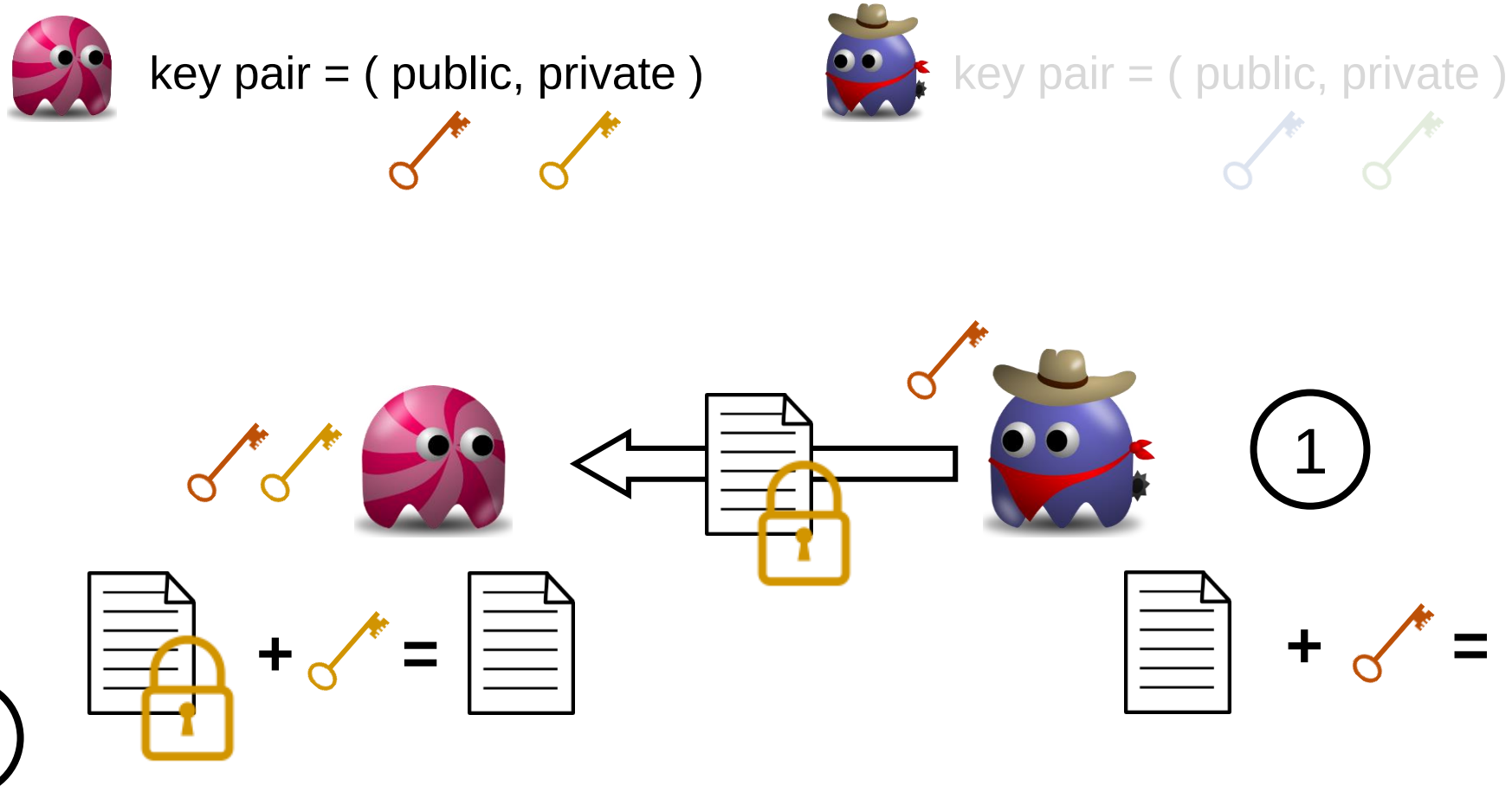
- Alice sends a message to Bob





Asymmetric Encryption: Confidentiality

and Bob responds

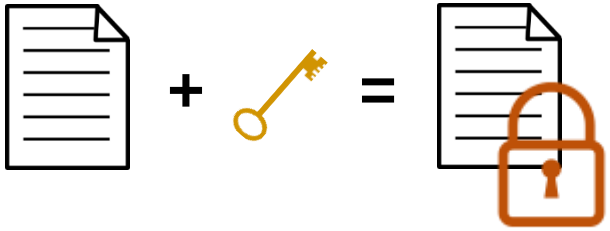


Asymmetric Encryption: Authentication

- Can be used to authenticate (sign)

key pair = (public, private)

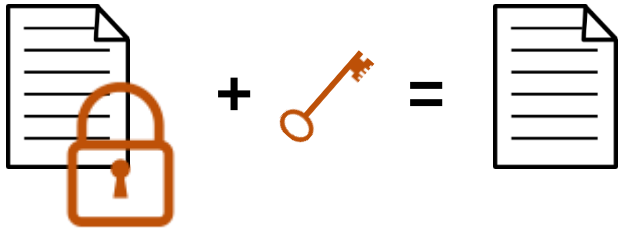
key pair = (public, private)



signs with her private key

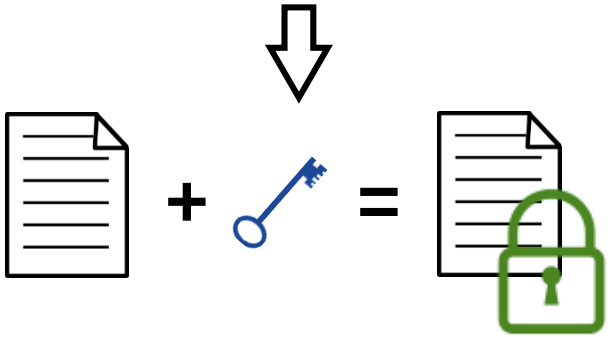
verifies with

public key

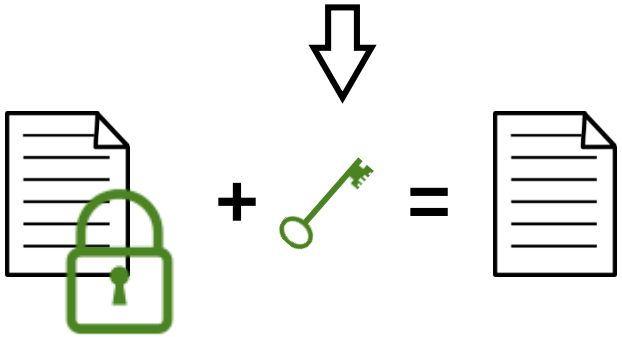


Asymmetric Encryption Cheat Sheet

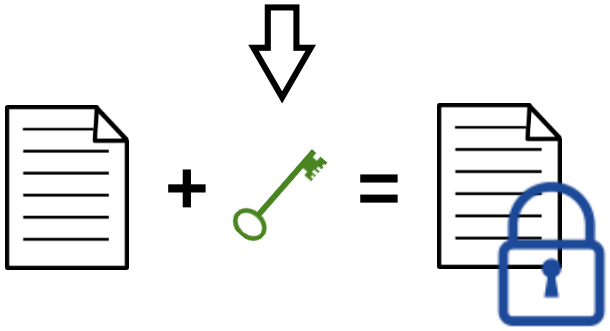
- Encrypts with Public Key



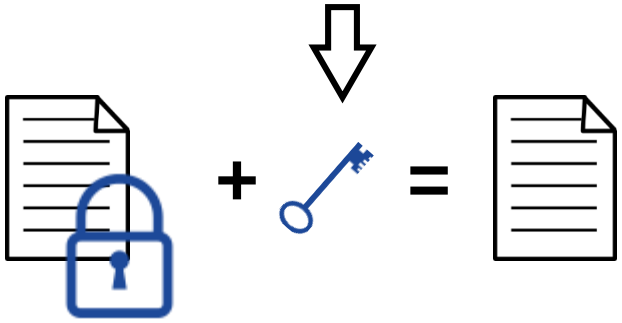
- Decrypts with Private Key



- Signs with Private Key



- Verifies with Public Key

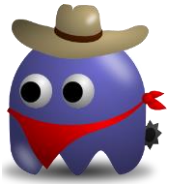


Symmetric + Asymmetric in Practice

- public key encryption + symmetric key encryption + hashing

private key

public key

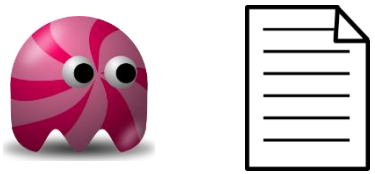


private key

public key

Symmetric + Asymmetric (PGP)

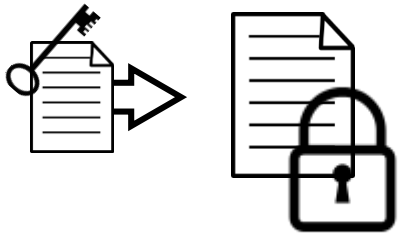
- public key and symmetric key encryption + hashing



1

generate random (symmetric) key

2



In practice (with PGP)

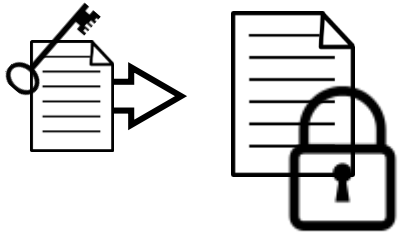
private key
public key

private key
public key

1

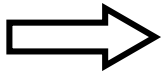
generate random
(symmetric) key

2



3

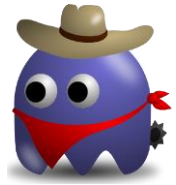
hash ( )



In practice (with PGP)

private key

public key



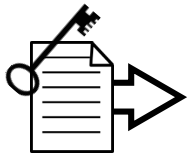
private key

public key

1

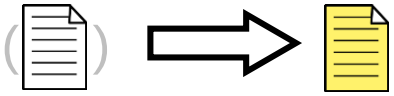
generate random (symmetric) key

2



3

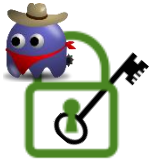
hash ( )



4

Enc( ) using

=



Sign( ) using

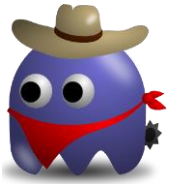
=

In practice (with PGP)

- Alice sends (2) and (4) to Bob

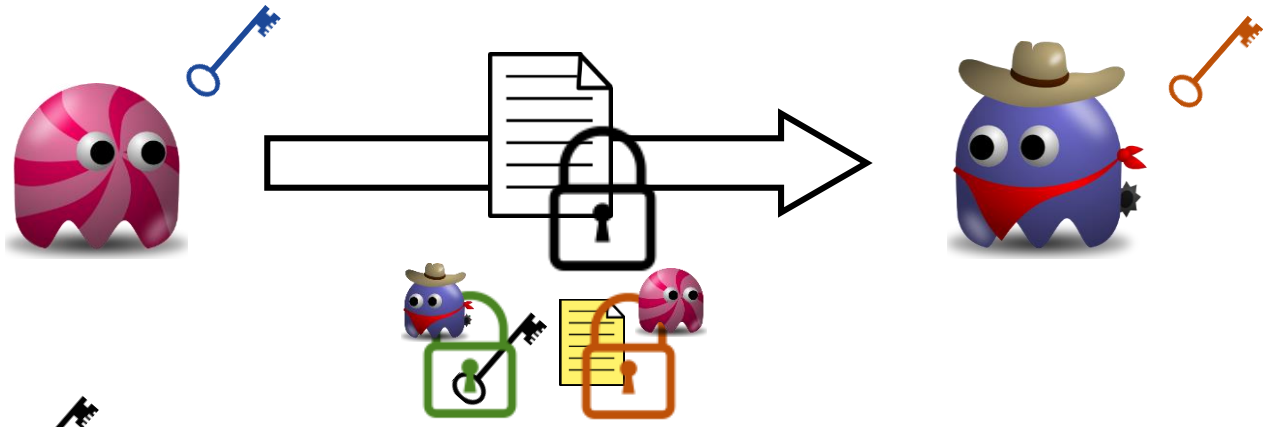
private key

public key



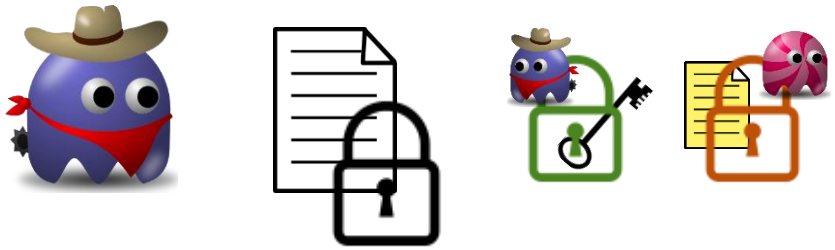
private key

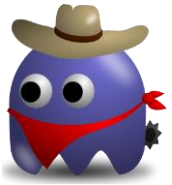
public key

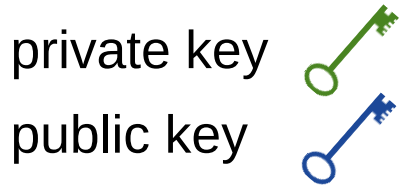


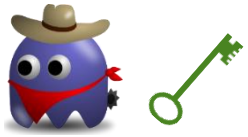
In practice (with PGP)

- public key and symmetric key encryption + hashing





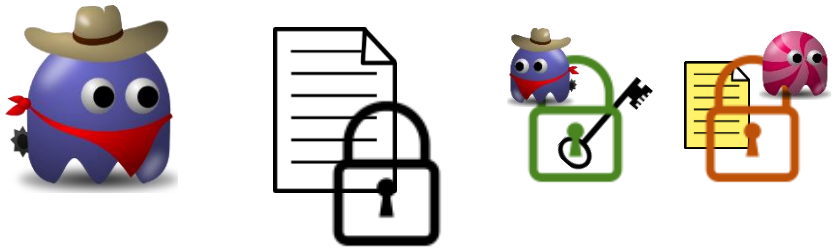


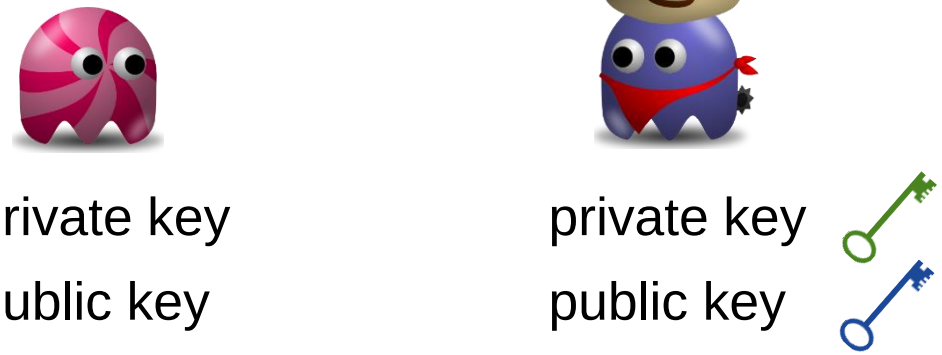
- Dec() using  =

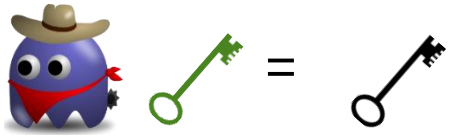
- Dec() using  =

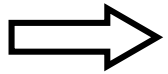
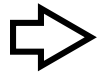
In practice (with PGP)

- public key and symmetric key encryption + hashing





- Dec() using  =

- hash()    equal?( ) 

- Dec() using  = 

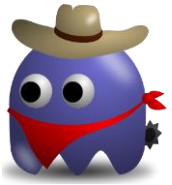
- Ver() using   = 

In practice (with PGP)

- public key and symmetric key encryption + hashing

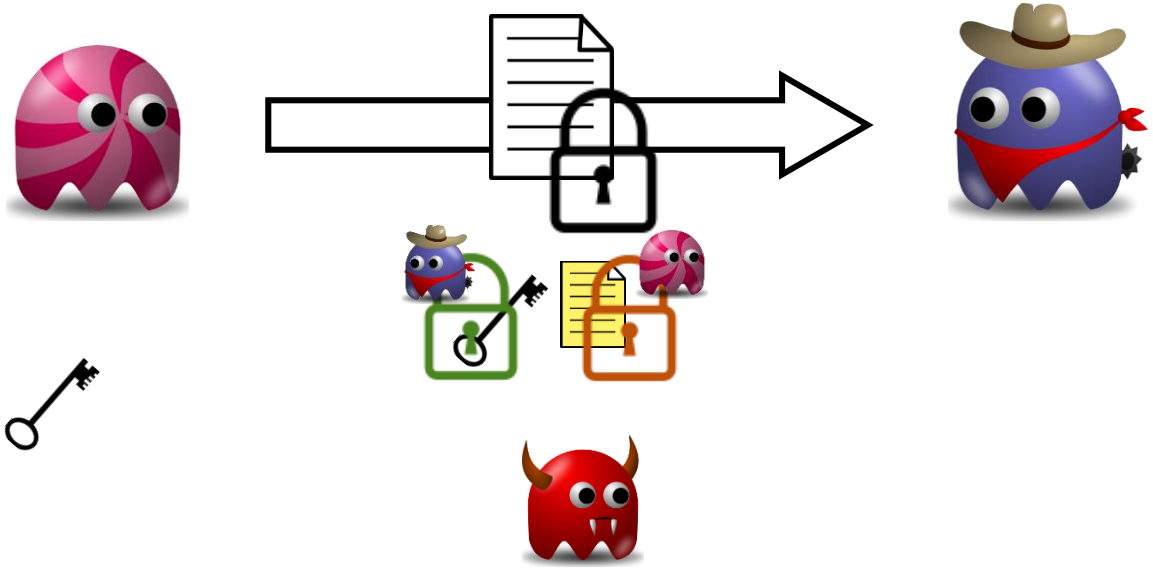
private key

public key



private key

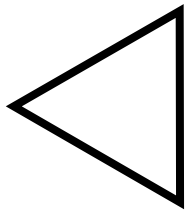
public key

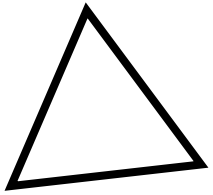


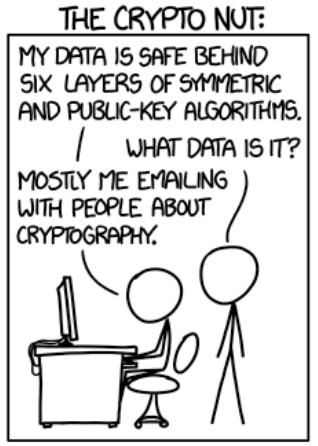
Computer and Network Security

Objectives:

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accounting

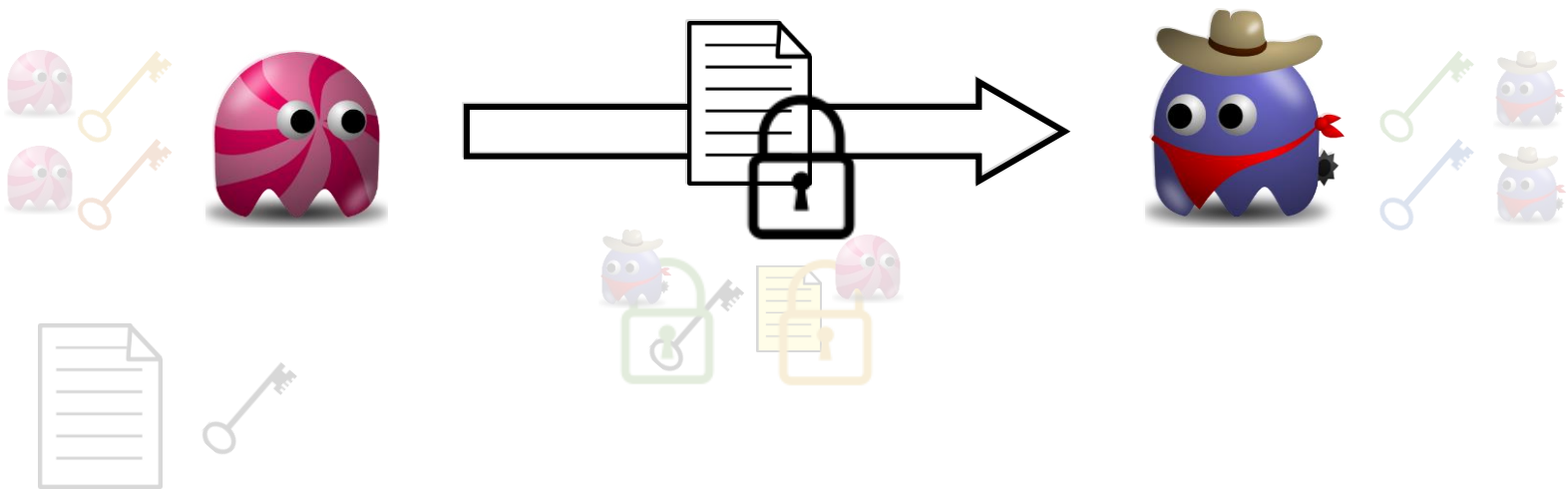






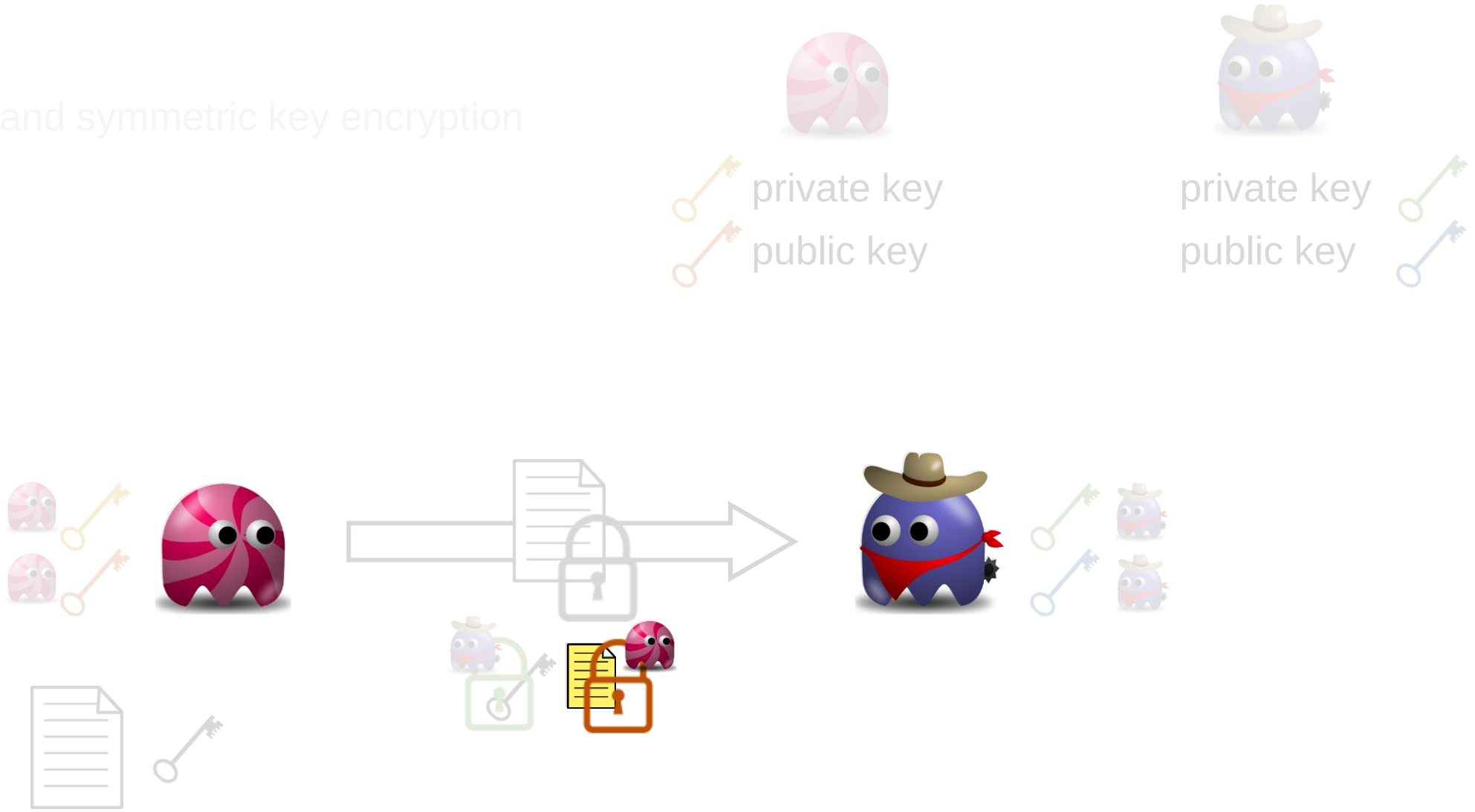
https://www.xkcd.com/1269/

Confidentiality



Integrity

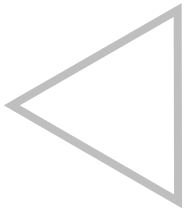
- public key and symmetric key encryption + hashing



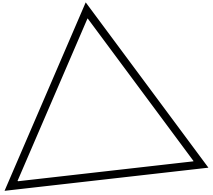
Computer and Network Security

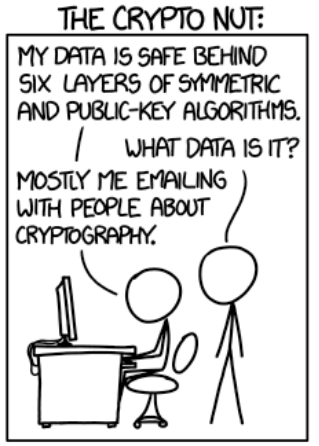
Objectives:

- Confidentiality
- Integrity
- Availability



- Authentication
- Authorization
- Accounting





https://www.xkcd.com/1269/

Authentication

Are you really who you claim to be?

How to prove it ?

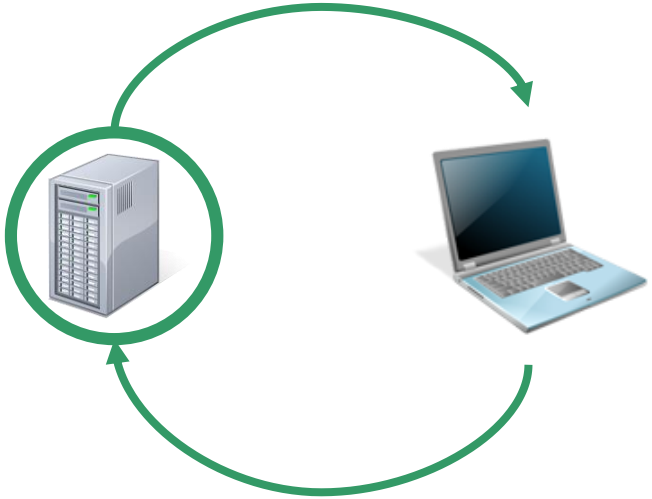
Authentication

Are you really who you claim to be?

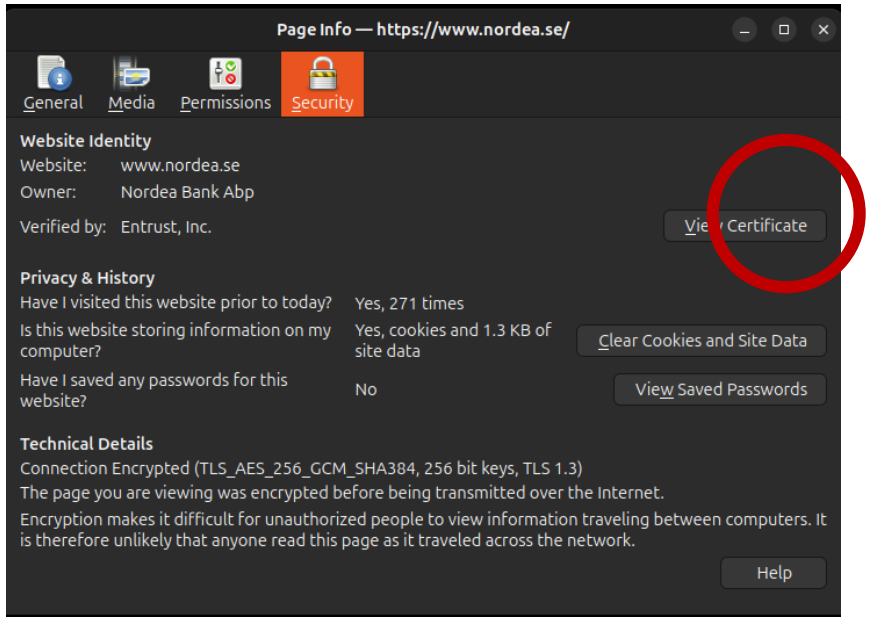
How to prove it ?

- something you know
- something you have
- something you are
- from a location

Authentication



- Digital certificates for secure connections
  - A given format: X.509 standard

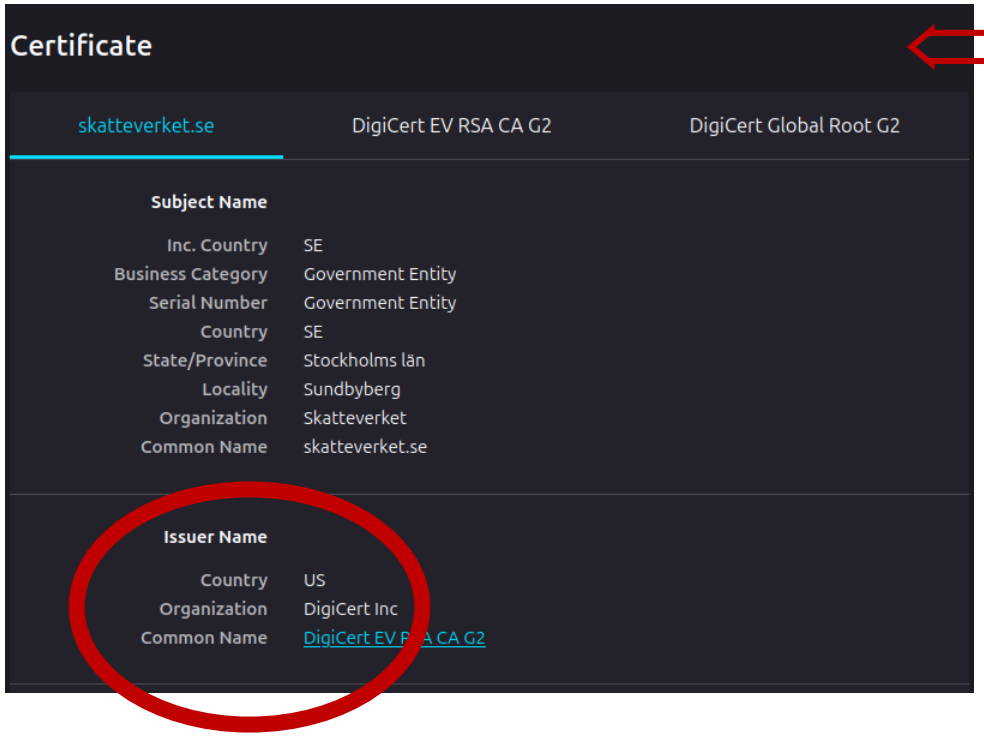


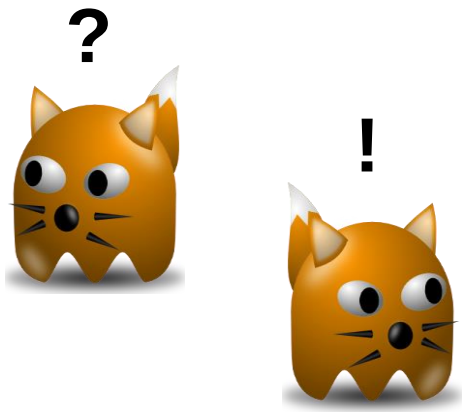
a signed public key
issued by the signer

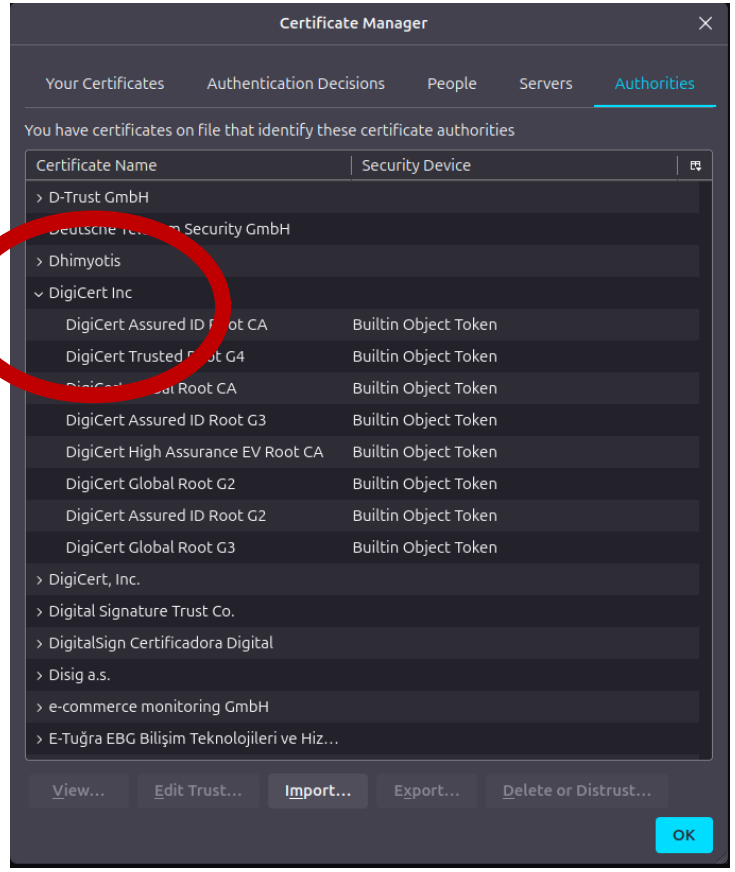
It requires a lot of infrastructure around it ➡ PKI

Certificates and Certificates Authorities

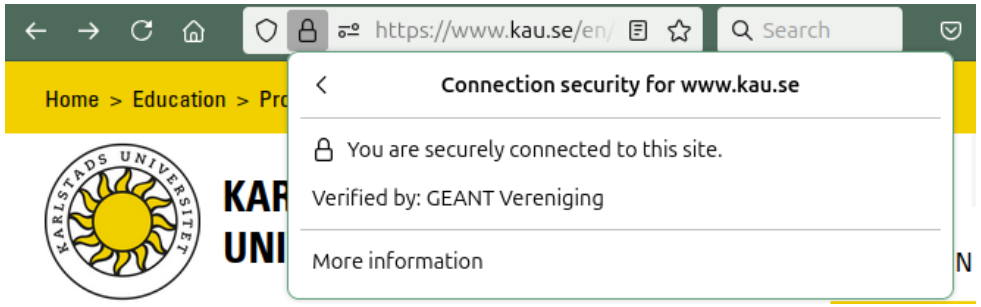
Trust me!







Digital Certificates



Certificate Policies

Policy	Statement Identifier (1.3.6.1.4.1)
Value	1.3.6.1.4.1.6449.1.2.2.79
Qualifier	Practices Statement (1.3.6.1.5.5.7.2.1)
Value	https://sectigo.com/CPS
Policy	Certificate Type (2.23.140.1.2.2)
Value	Organization Validation

- different types:
  - domain validation (DV)

Certificate Policies

Policy	Certificate Type (2.23.140.1.2.1)
Value	Domain Validation

  - organization validation (OV)
  - extended validation (EV)

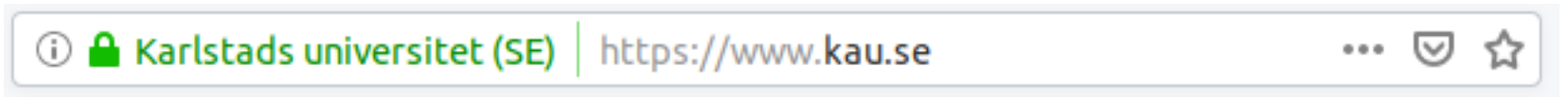
Certificate Policies

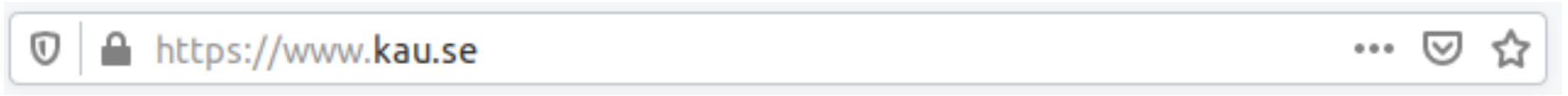
Policy	ANSI Organizational Identifier (2.16.840)
Value	2.16.840.1.114412.2.1
Policy	Certificate Type (2.23.140.1.1)
Value	Extended Validation
Qualifier	Practices Statement (1.3.6.1.5.5.7.2.1)
Value	http://www.digicert.com/CPS

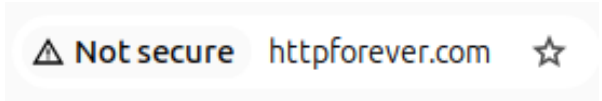
Authentication

- Is this good authentication?

What about these?



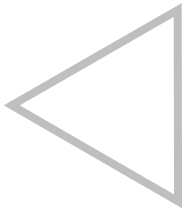




Computer and Network Security

Objectives:

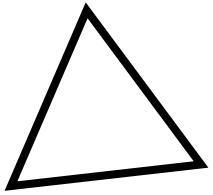
- Confidentiality
- Integrity
- Availability

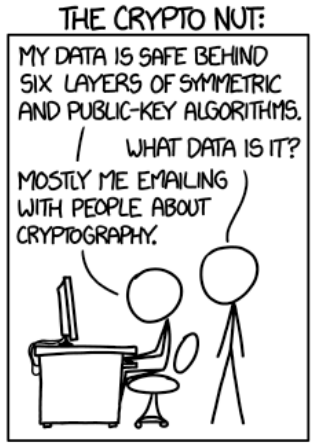


- Authentication

⬇

- Authorization
- Accounting



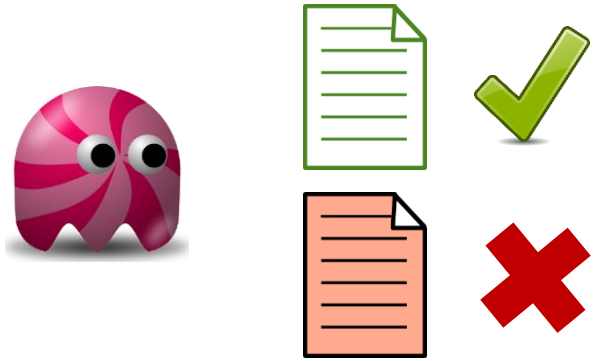


https://www.xkcd.com/1269/

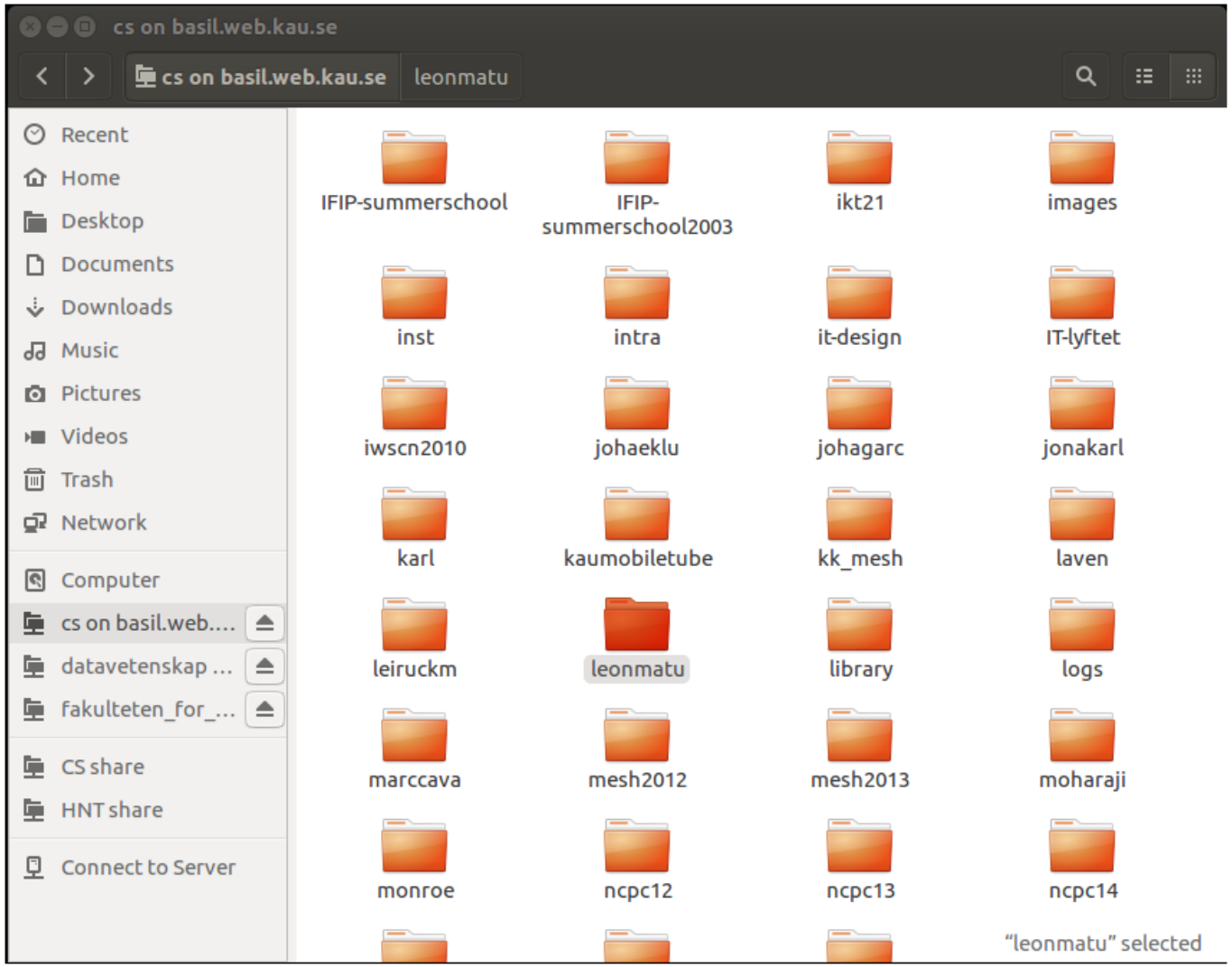
Authorization

- IF authentication is positive 

authorization for deciding on rights



Authorization needs Access Control



what can  access ?
what can she not ?

(find out more in D23 !)

What Have You Seen Today ?

Definitions:

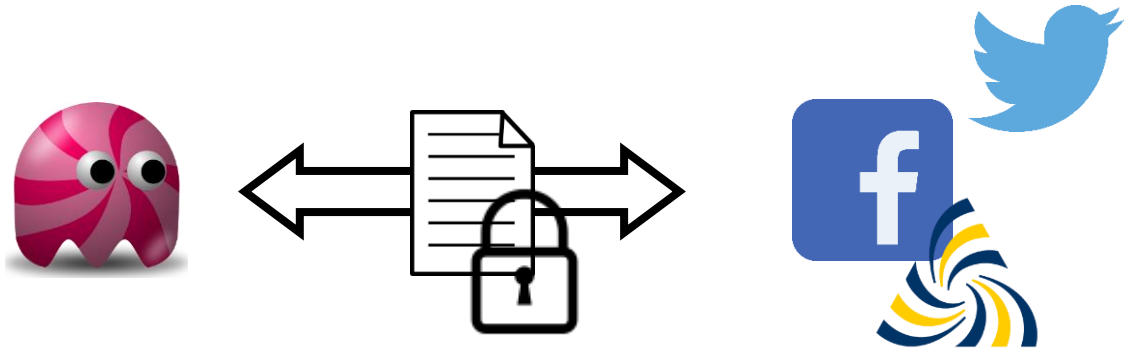
- Confidentiality
- Integrity
- Availability

- Authentication
- Authorization
- Accounting

+ Symmetric and Asymmetric keys
+ Hash functions

+ Examples

It’s Everywhere



Next

1. Introduction to the Course
2. Security Fundamentals (x2)
3. Network Security
4. Firewalls
5. Security at ICA-Gruppen
6. Intrusion Detection
7. Privacy, Security and Ethics
8. Design Principles
9. Web Security
10. Risk Analysis
11. Software Security (x2)
12. Pen Testing

Assignment 1

Assignment 2

Assignment Questions

Questions 1-3

Q1. What does confidentiality provide? How can confidentiality be obtained in a computer system?

Q2. What is the difference between authentication and authorization?

Q3. In the following scenarios, explain what type of security violations are present (if any).

a. Eve () crashes the course webpage 

b. Alice () crashes the course webpage

c. Eve () changes the amount of Bob's phone invoice  

d. Eve () shoulder surfs Alice's password to the C19 course and logs in as Alice 

Questions 4-5

Q4. How would you compare symmetric to asymmetric encryption in terms of:

a. how many keys would Alice and Bob need to communicate in each case?

b. how many keys are needed for *n* participants to communicate?

d. key distribution?

c. computational performance?

Q5. Explain how does authenticated encryption functions provide both authentication and encryption.