

Security Fundamentals

DVGC19



KARLSTAD
UNIVERSITY
SWEDEN

Leonardo A. Martucci

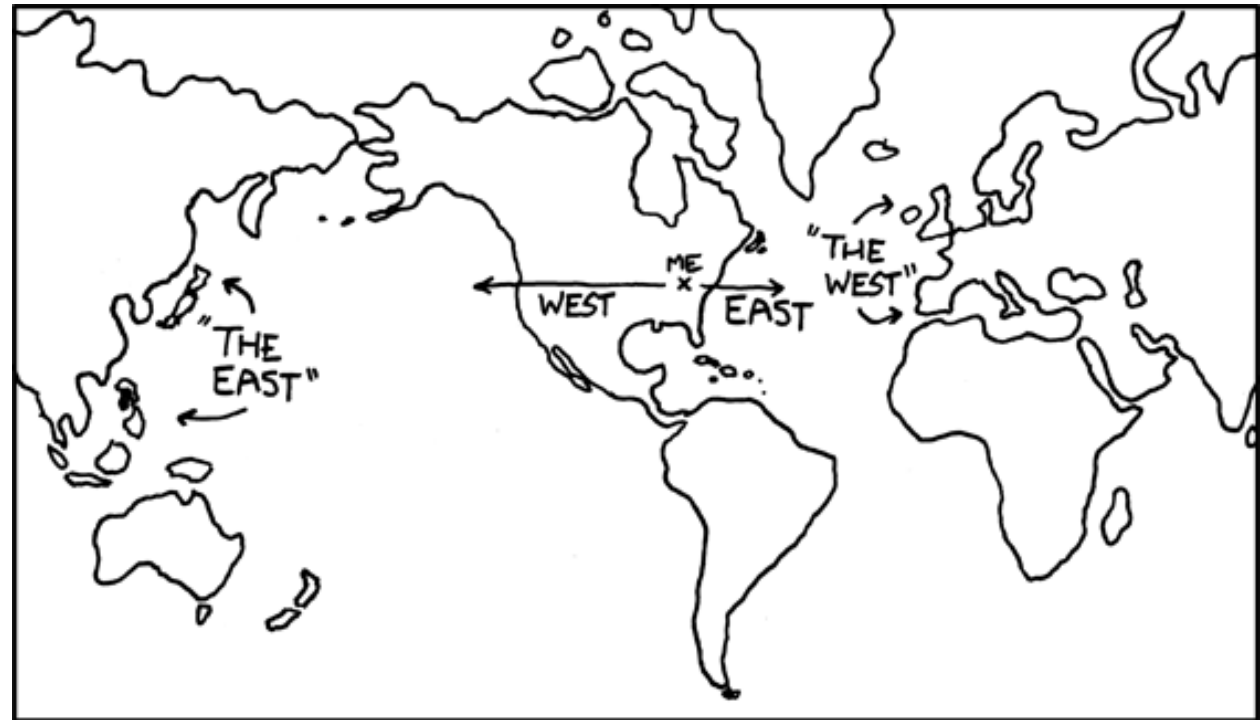
Lectures

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



THIS ALWAYS BUGGED ME.

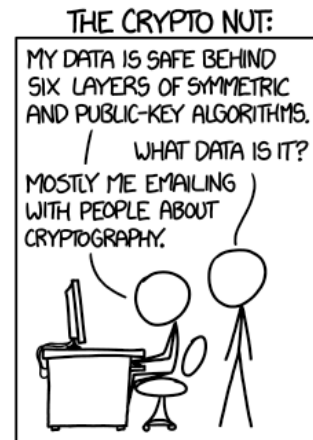
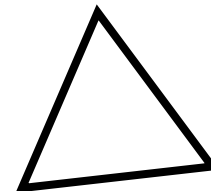
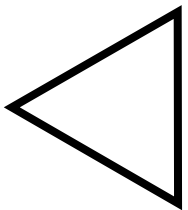
OPINIONS ON INTERNET PRIVACY



Computer and Network Security

Objectives:

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

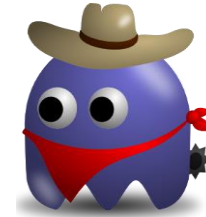


The Actors

- Alice



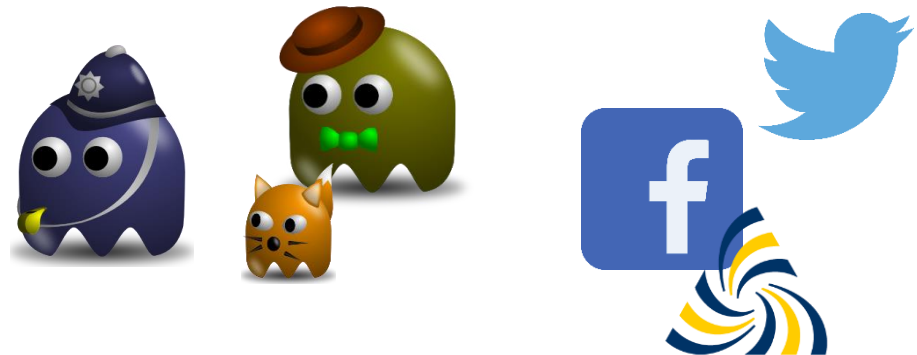
- Bob



- Eve (Mallory)



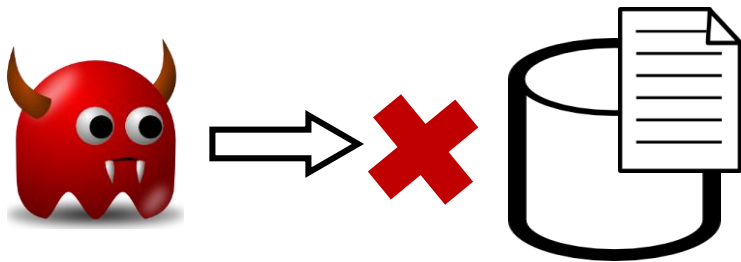
(+ The Support Cast)



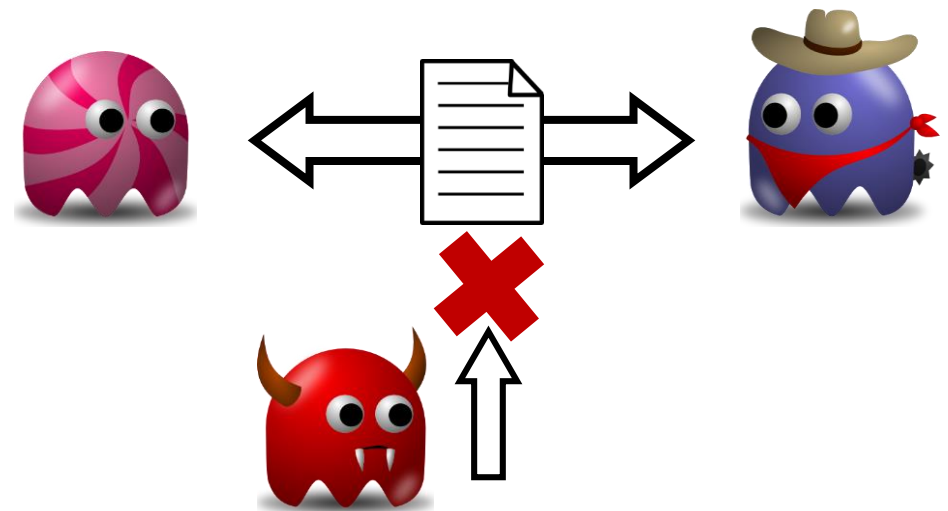
Confidentiality

- Information NOT available or disclosed to unauthorized parties

- Stored Data



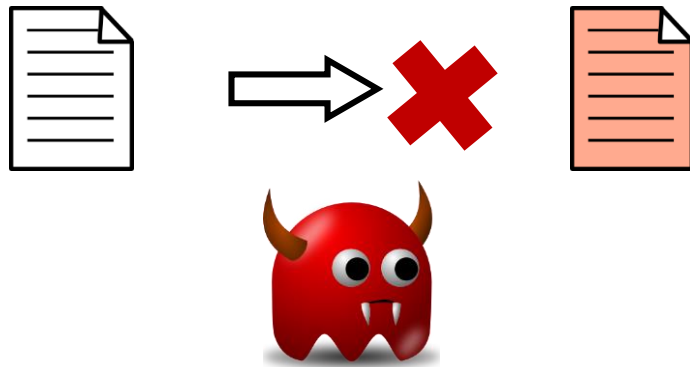
- Data in Transit



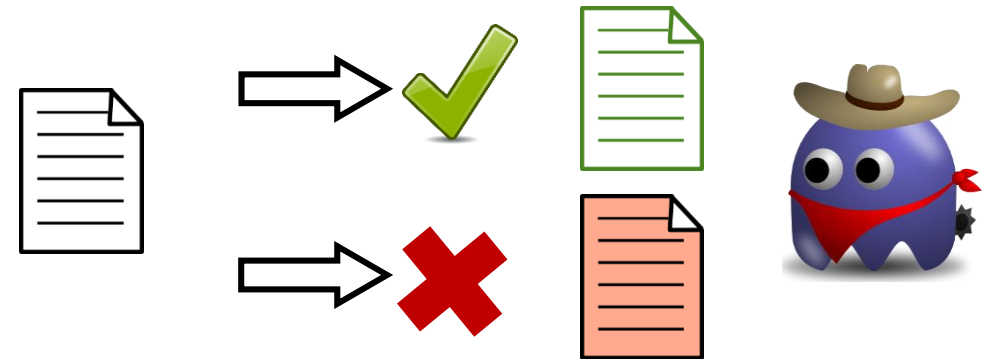
Integrity

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

- Unauthorized Parties



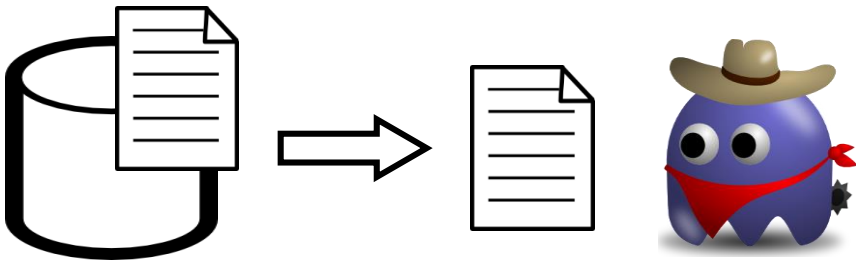
- Unauthorized Manner



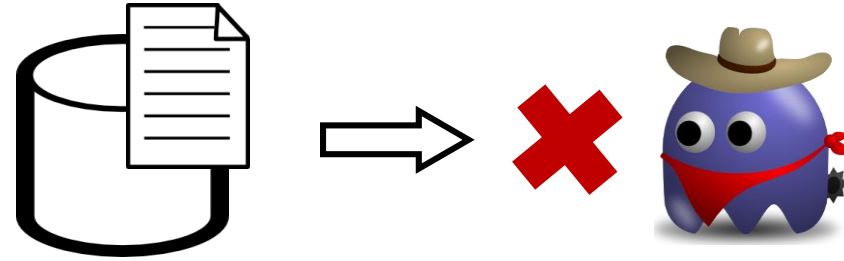
Availability

- Information available when needed

- Available



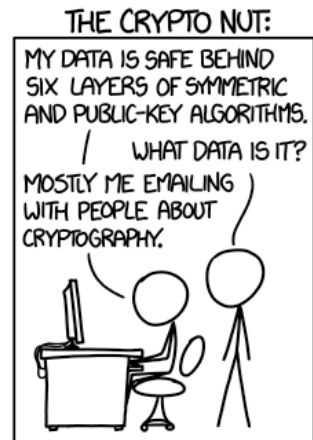
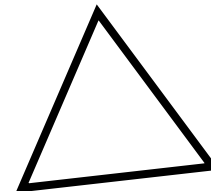
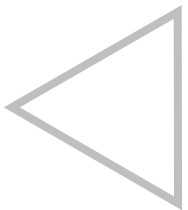
- NOT Available



Computer and Network Security

Objectives:

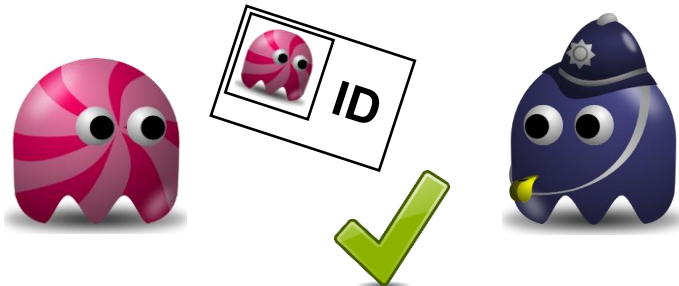
- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accounting



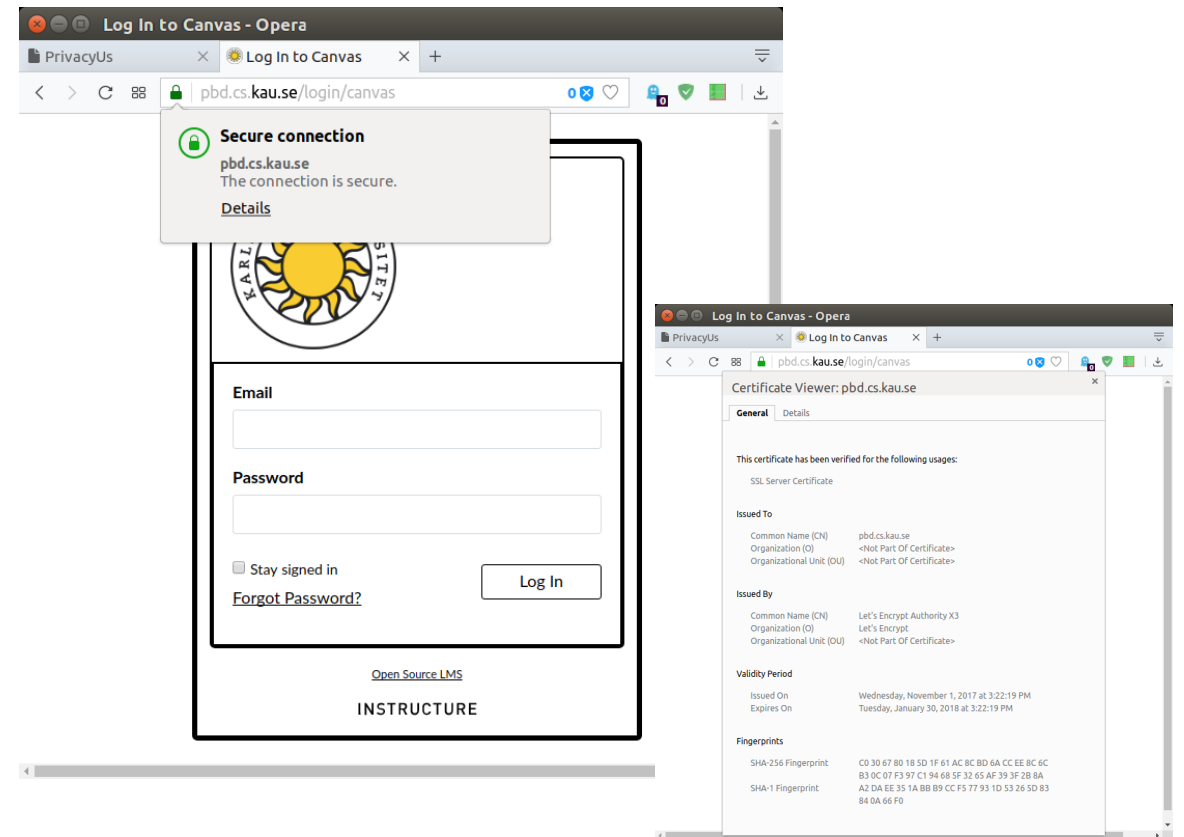
Authentication

- Assurance of an identity claim
Are you really who you claim to be?

- ID cards



- Digital certificates

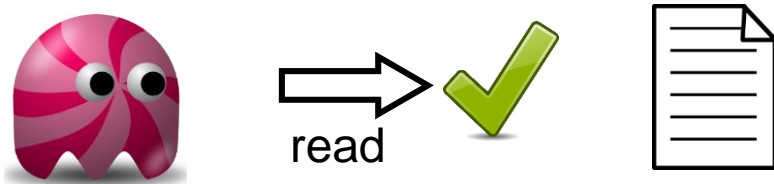


Authorization

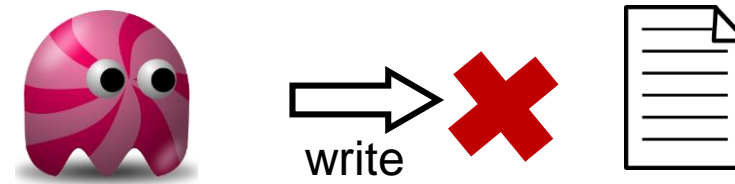
- Grant or deny access to resources
operations over resources
(once authenticated)



- Authorized



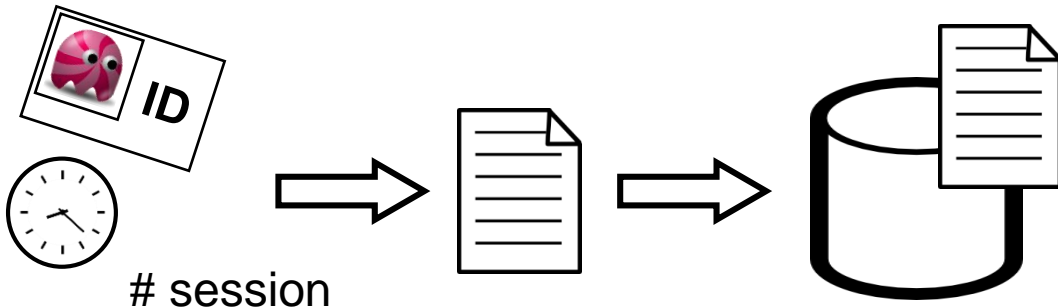
- NOT Authorized



Accounting

- Keeping track of information
users and data

- Building and storing log data



Cryptomagic



Building Blocks

- message



- cyphertext



- encryption function $\Rightarrow e ()$

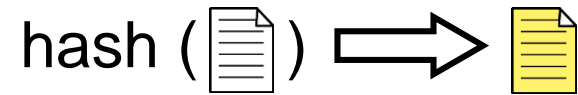
- decryption function $\Rightarrow d ()$



- key(s)



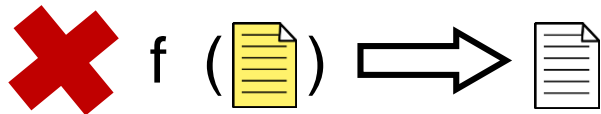
Hash Functions

- A one-way function



 = message (arbitrary)
 = digest (fixed length)

meaning:



+ a number of security properties (C20!)

Building Blocks

- message




- cyphertext



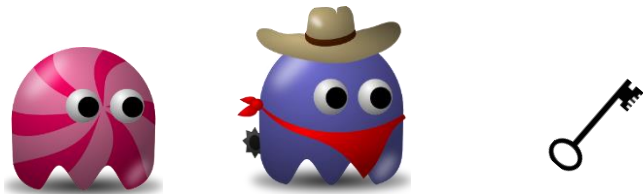
- encryption function $\Rightarrow e ()$

- decryption function $\Rightarrow d ()$

- key(s) 

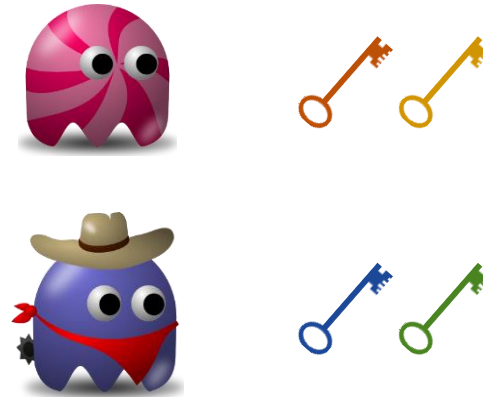
Algorithms and Keys

symmetric





- 1 (shared) key

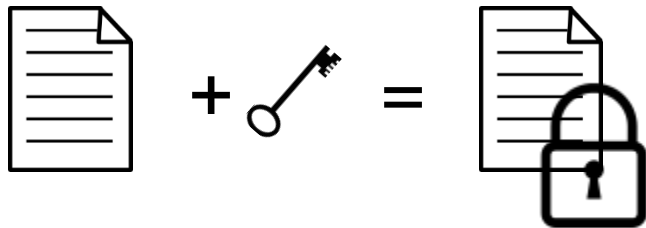
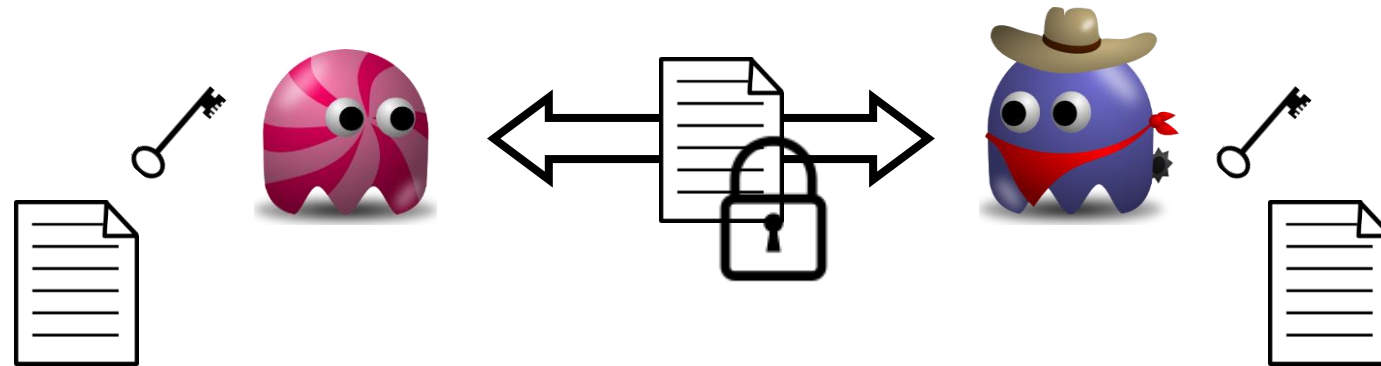
asymmetric



- 2 key pairs

Symmetric Encryption

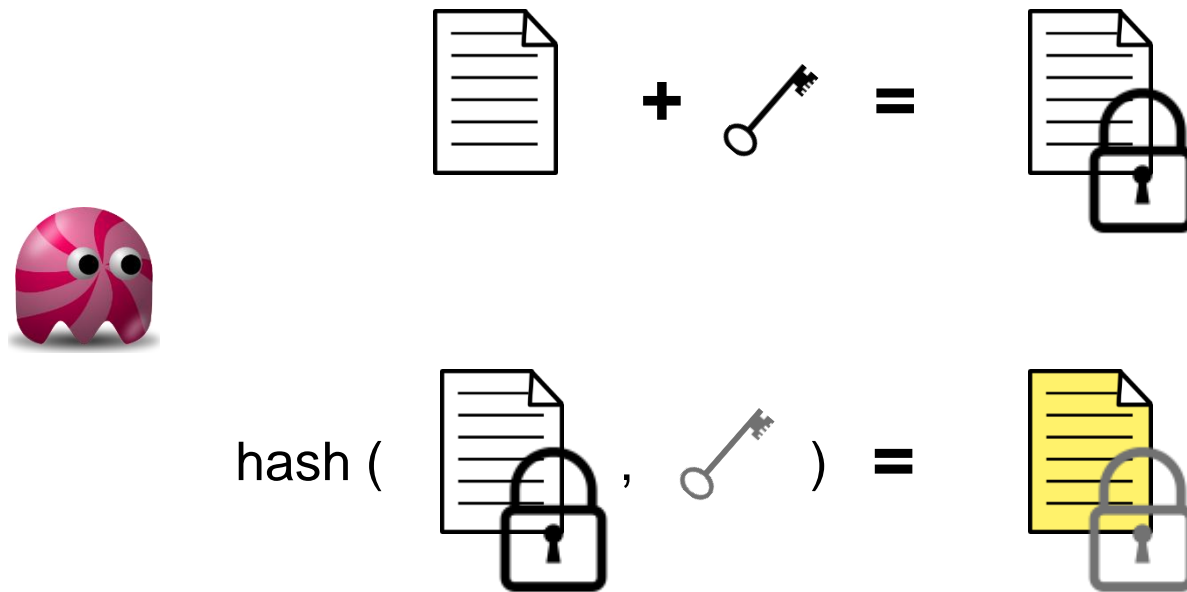
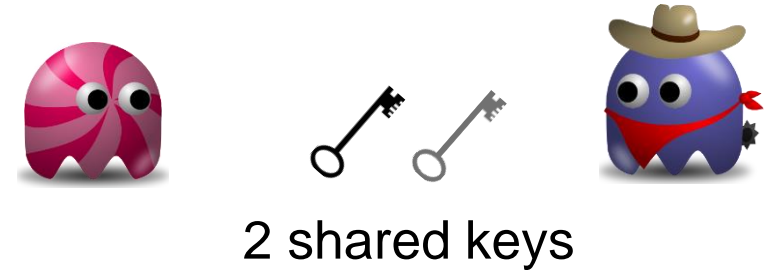
- Alice & Bob  1 shared key 



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

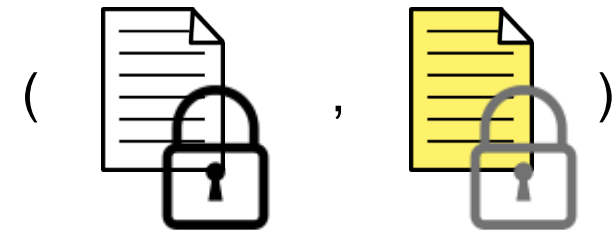
Symmetric Encryption in Practice

- with symmetric keys:
authenticated encryption (EtM)



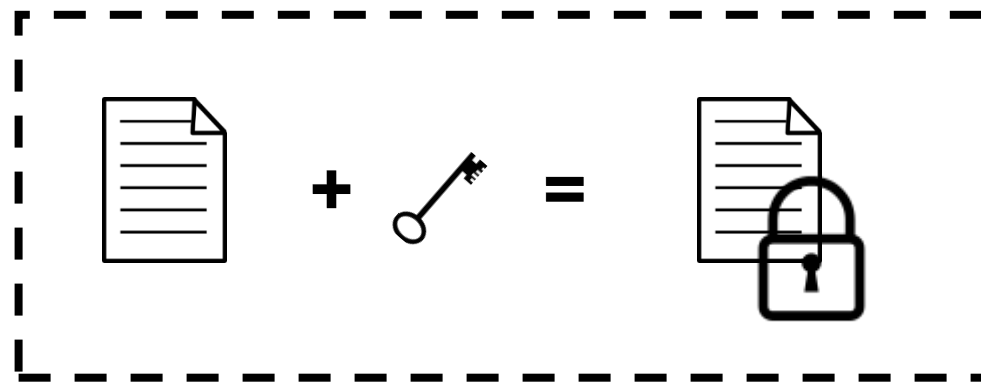
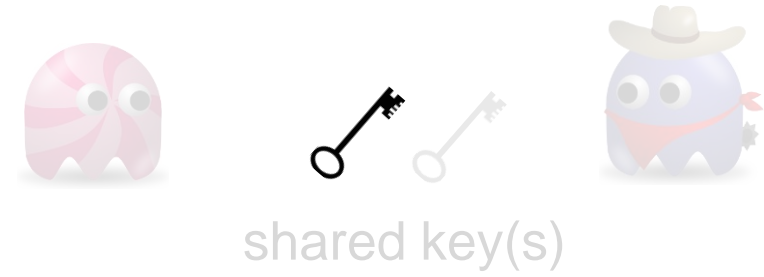
* keyed hash

encrypt-then-MAC message



Symmetric Encryption in Practice

- with symmetric keys:
authenticated encryption (EtM)



⇒ symmetric encryption

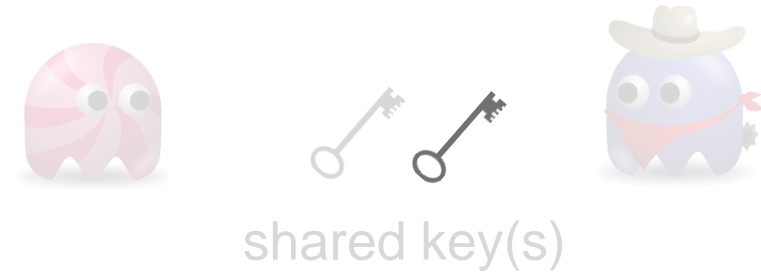
encrypt-then-MAC message



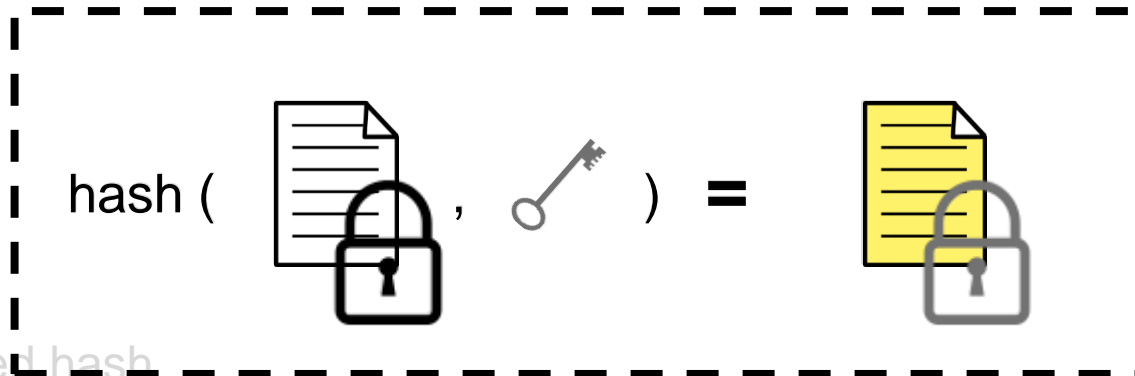
* keyed hash

Symmetric Encryption in Practice

- with symmetric keys:
authenticated encryption (EtM)



encrypt-then-MAC message



* keyed hash

authentication

Asymmetric Encryption

- Alice & Bob  2 key pairs



key pair = (public, private)



key pair = (public, private)



Asymmetric Encryption: Confidentiality

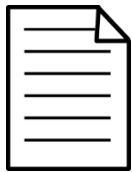
- For encryption and decryption



key pair = (public, private)



key pair = (public, private)



+



=



encrypts with



public key



decrypts with his private key



+



=

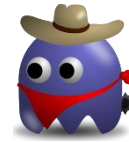


Asymmetric Encryption: Confidentiality

- Alice sends a message to Bob



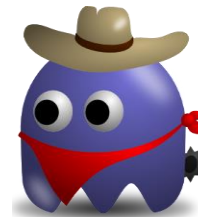
key pair = (public, private)



key pair = (public, private)



1



+



=



2



+



=



Asymmetric Encryption: Confidentiality

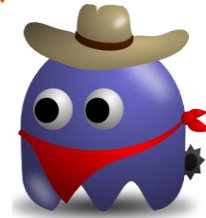
and Bob responds



key pair = (public, private)



key pair = (public, private)



1



+



=



+



=



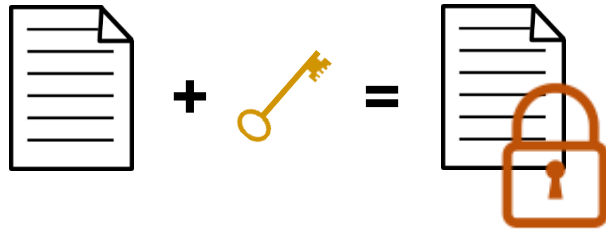
2

Asymmetric Encryption: Authentication

- Can be used to authenticate (sign)



key pair = (public, private)



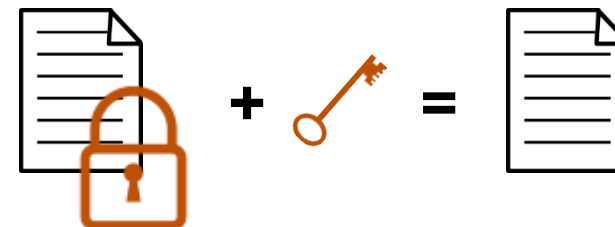
signs with her private key



key pair = (public, private)

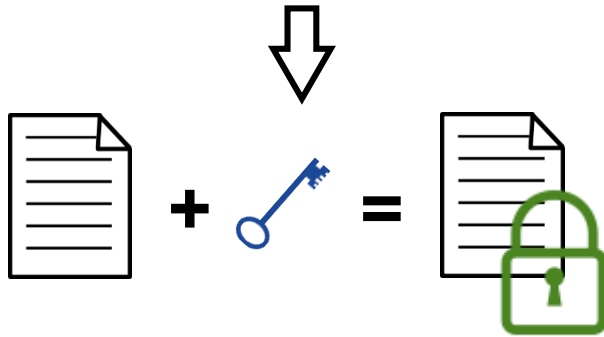


verifies with public key

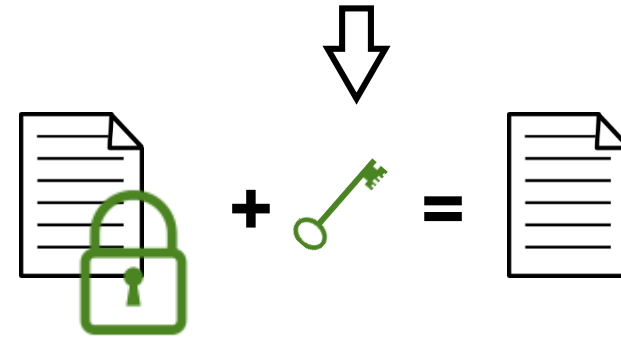


Asymmetric Encryption Cheat Sheet

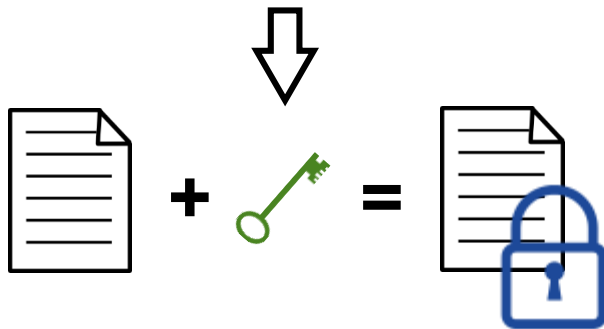
- Encrypts with Public Key



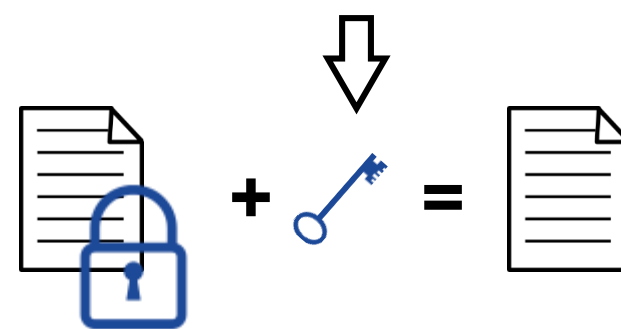
- Decrypts with Private Key



- Signs with Private Key

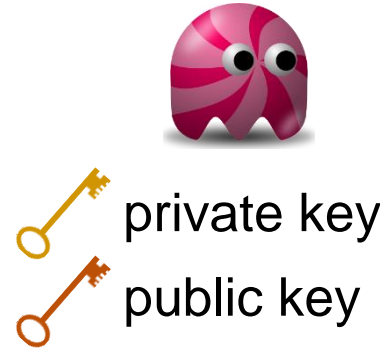


- Verifies with Public Key



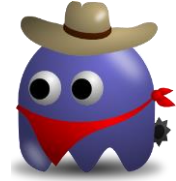
Symmetric + Asymmetric in Practice

- public key encryption + symmetric key encryption + hashing



private key

public key



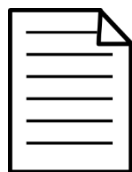
private key

public key



Symmetric + Asymmetric (PGP)

- public key and symmetric key encryption + hashing



1

generate random
(symmetric) key



2



private key

public key

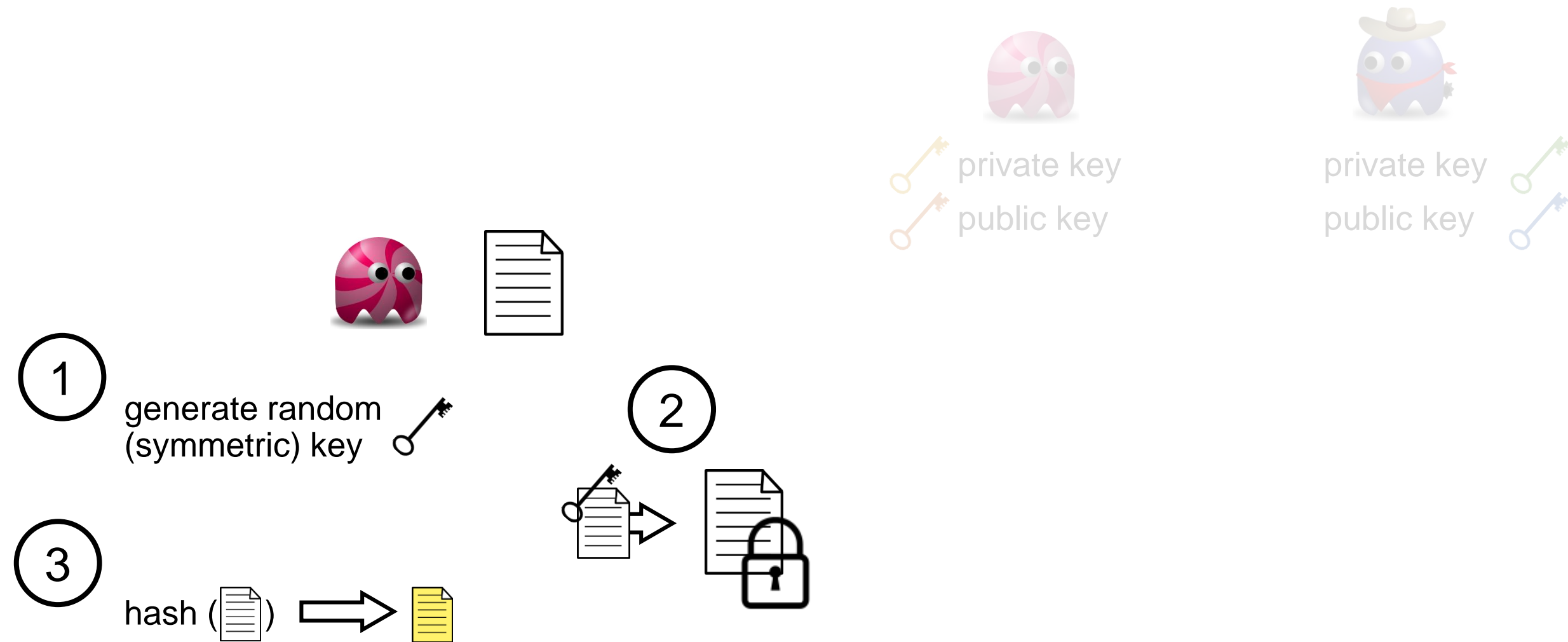


private key

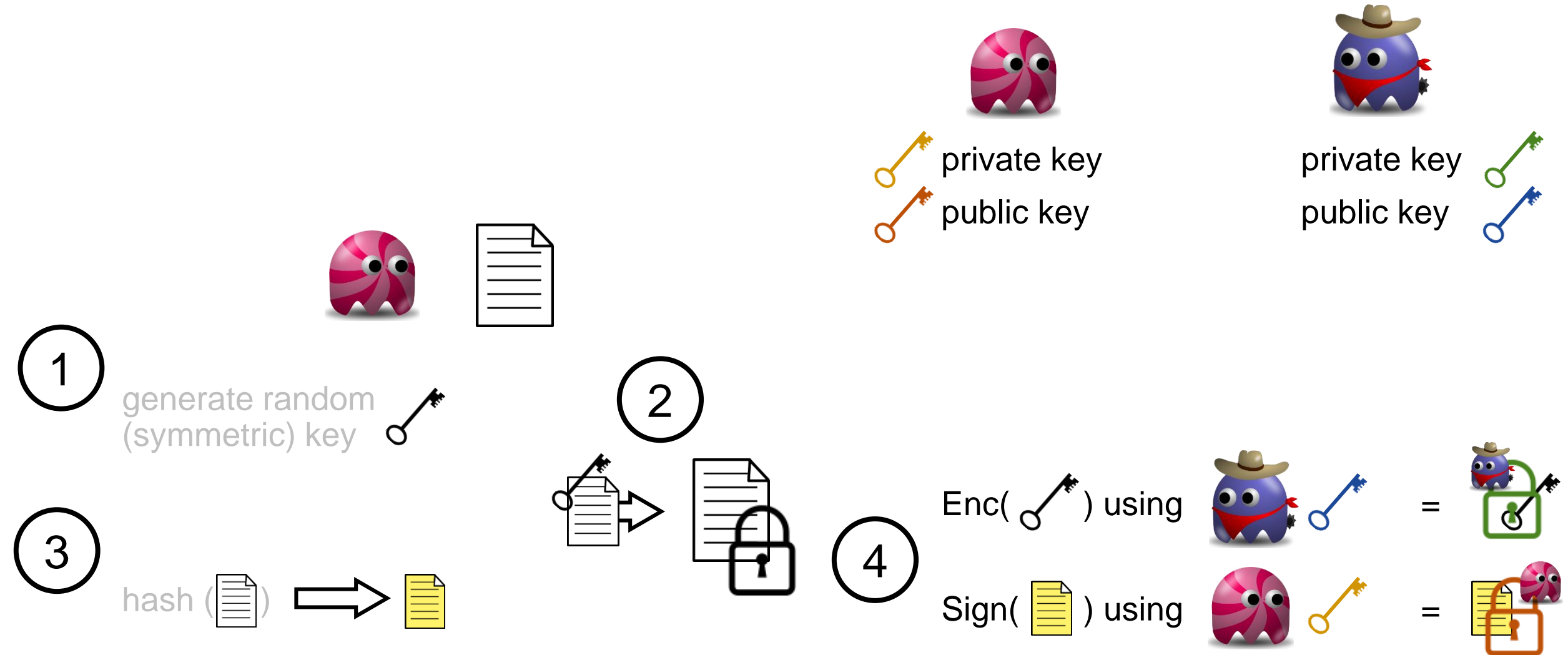
public key



In practice (with PGP)

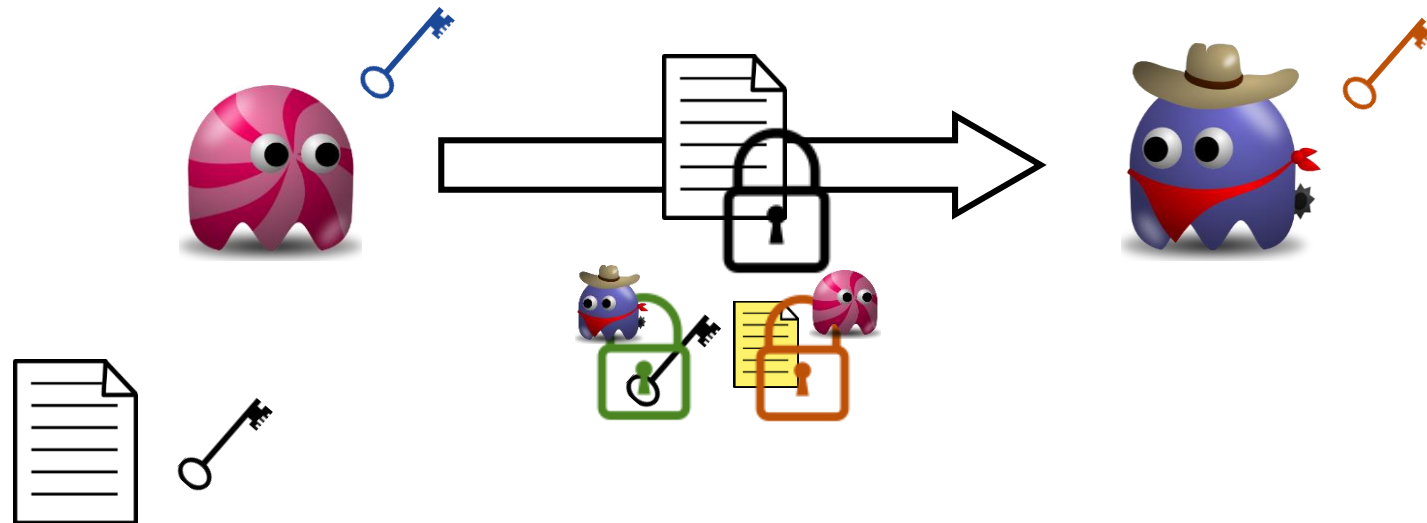
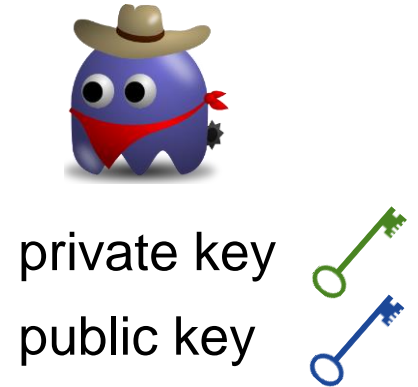


In practice (with PGP)



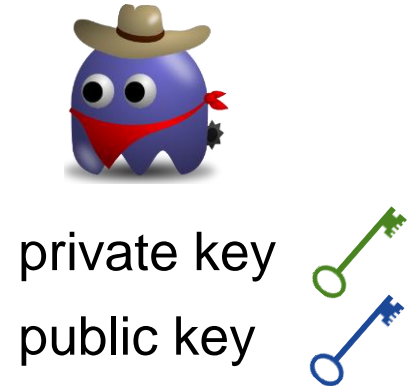
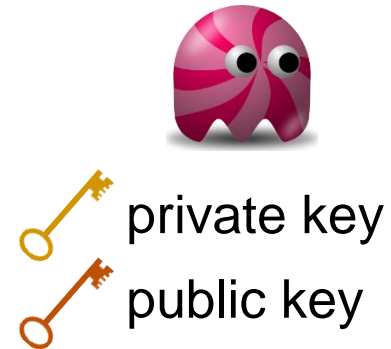
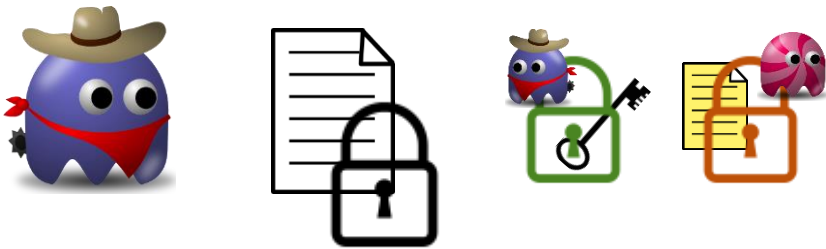
In practice (with PGP)

- Alice sends ② and ④ to Bob



In practice (with PGP)

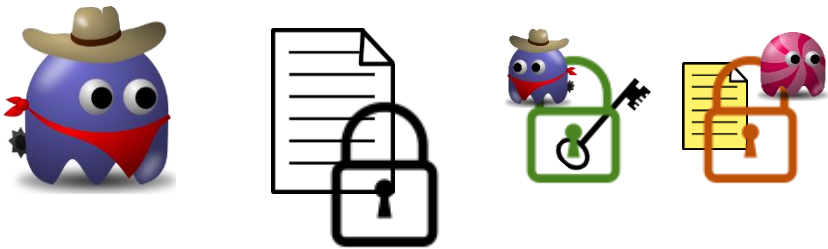
- public key and symmetric key encryption
+ hashing




- $\text{Dec}(\text{document with green lock})$ using blue private key = document
- $\text{Dec}(\text{document with padlock})$ using $\text{yellow private key}$ = document

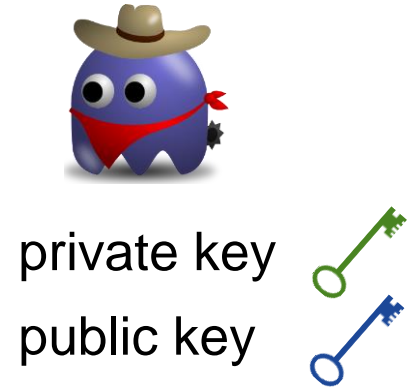
In practice (with PGP)





- public key and symmetric key encryption
+ hashing





- Dec() using   = 

- Dec() using  = 

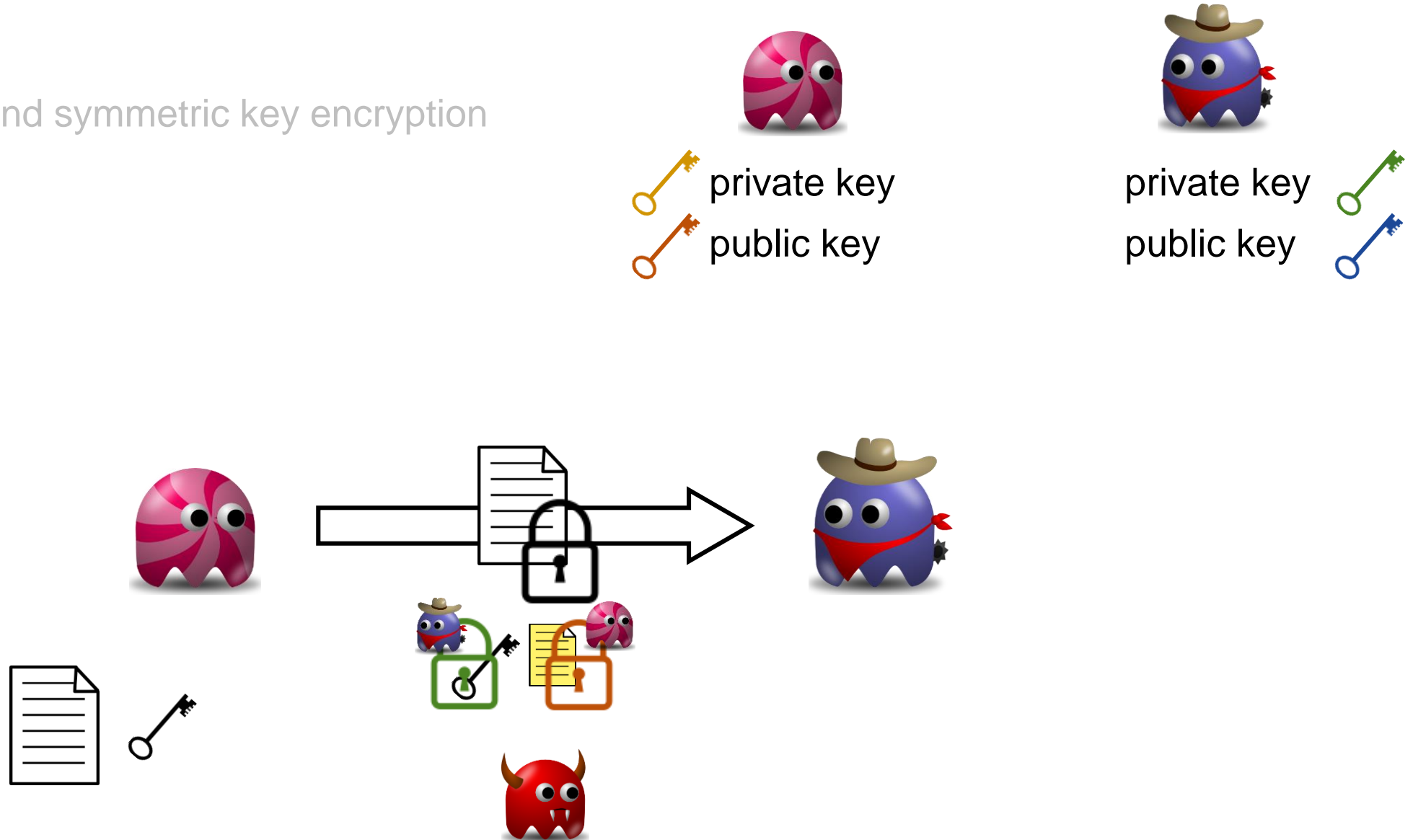


- hash() \Rightarrow  \Rightarrow equal?() 

- Ver() using   = 

In practice (with PGP)

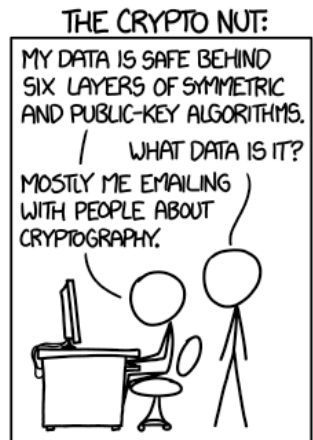
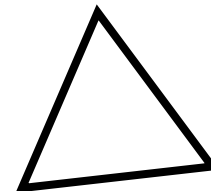
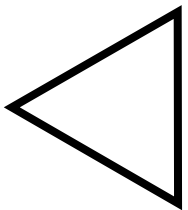
- public key and symmetric key encryption
+ hashing



Computer and Network Security

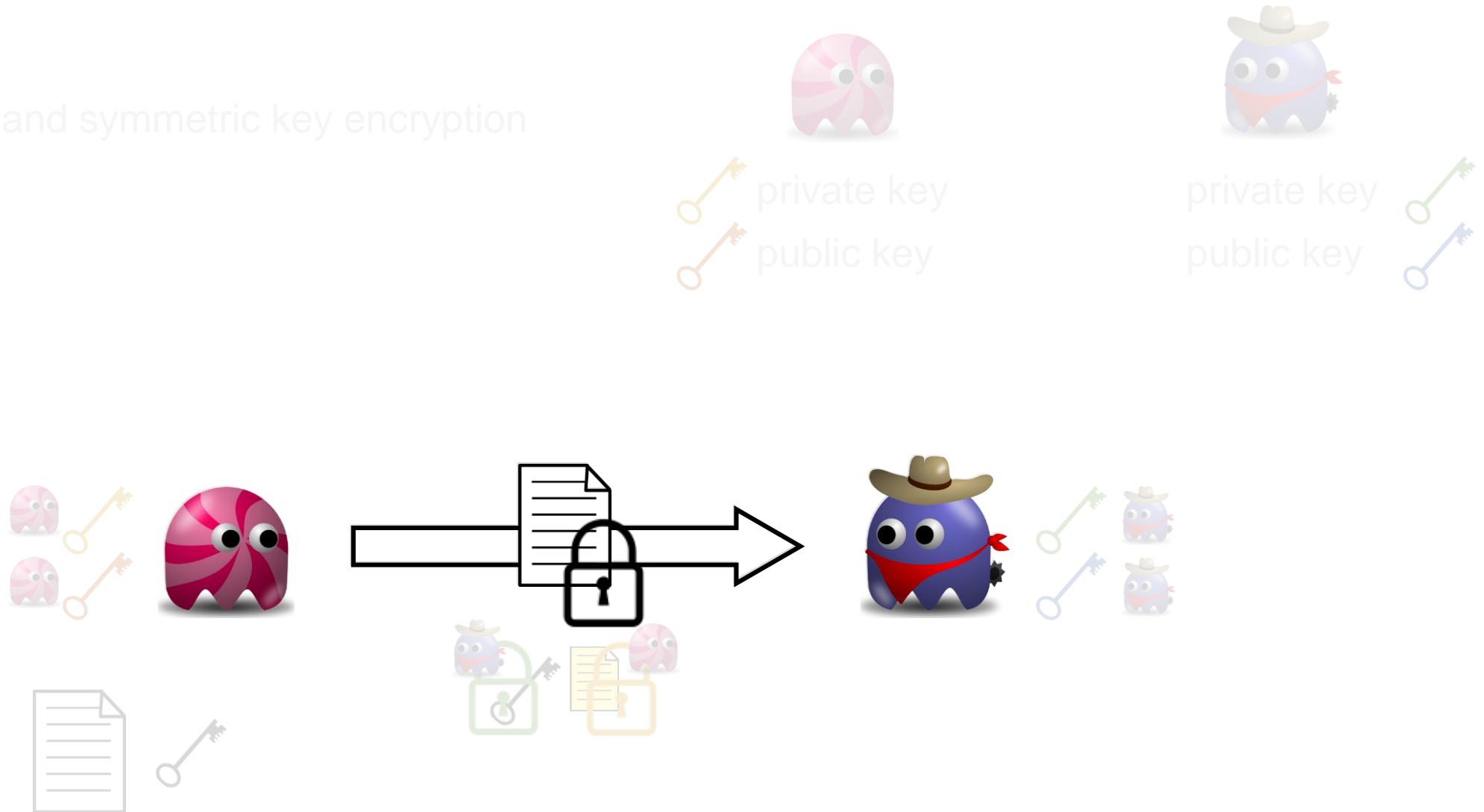
Objectives:

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



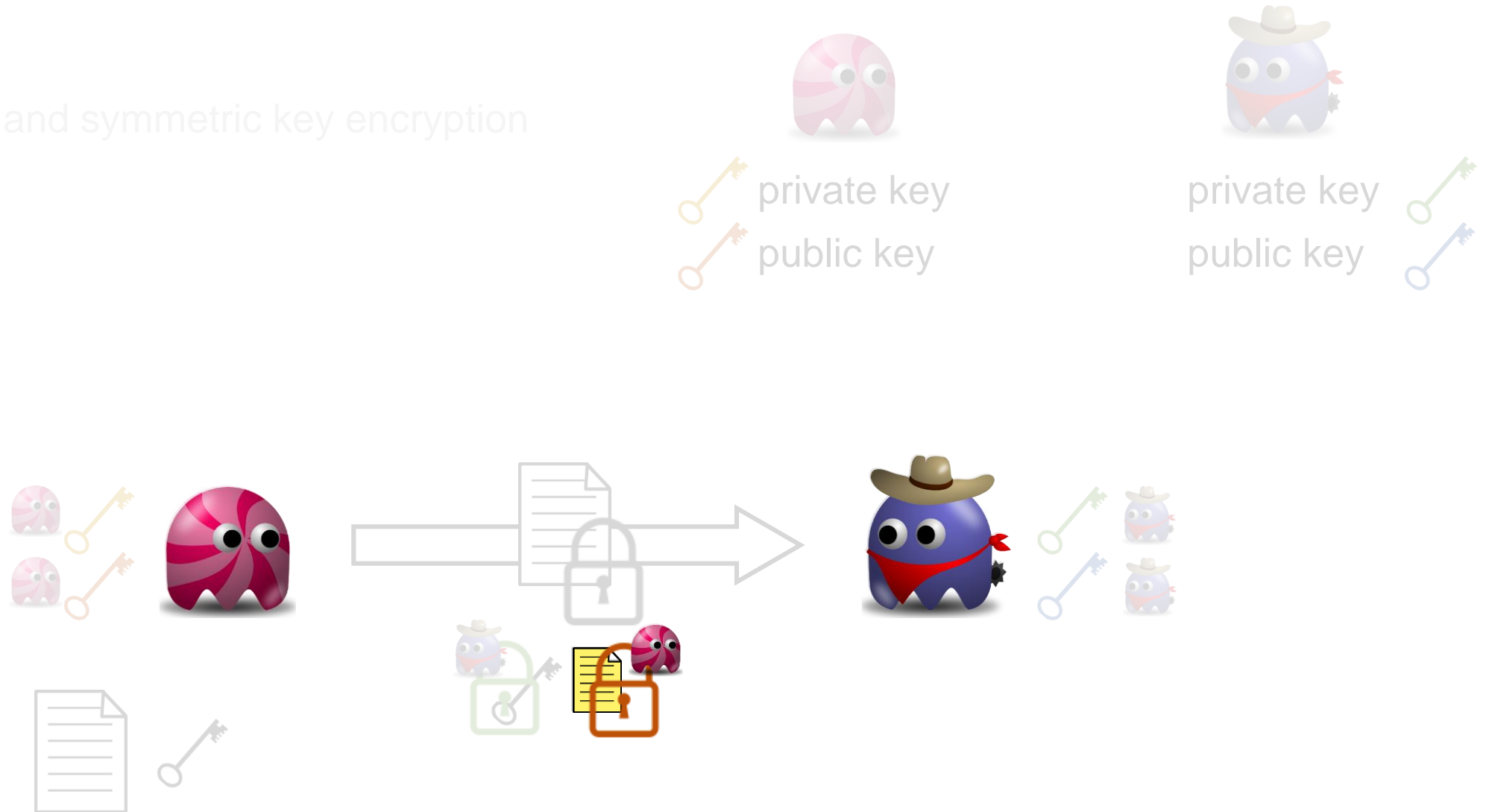
Confidentiality

- public key and symmetric key encryption
+ hashing



Integrity

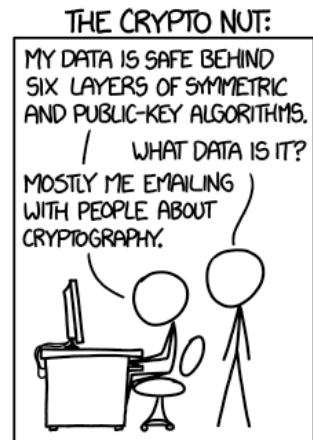
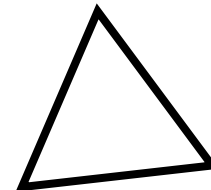
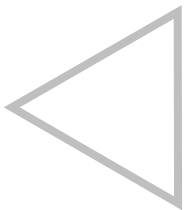
- public key and symmetric key encryption
+ hashing



Computer and Network Security

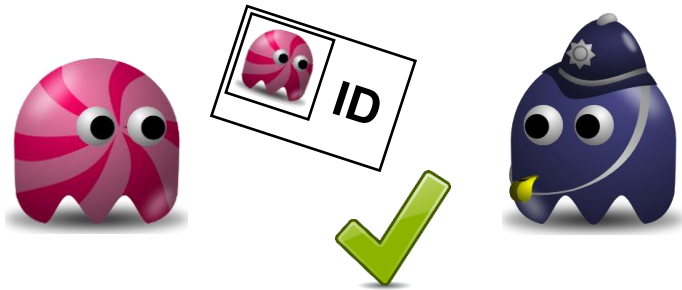
Objectives:

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



Authentication

Are you really who you claim to be?



How to prove it ?

Authentication

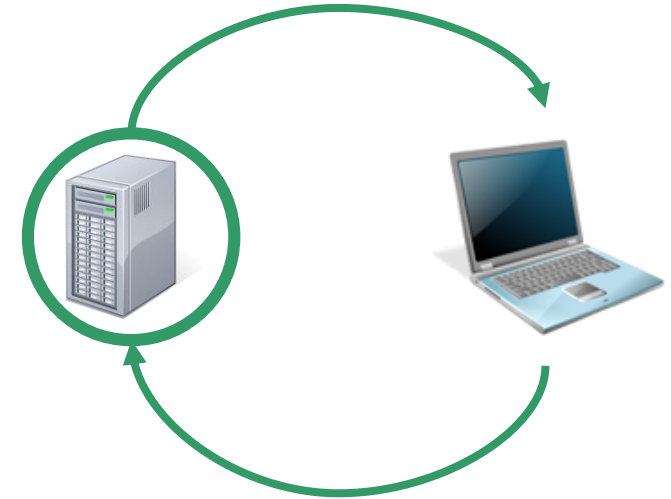
Are you really who you claim to be?



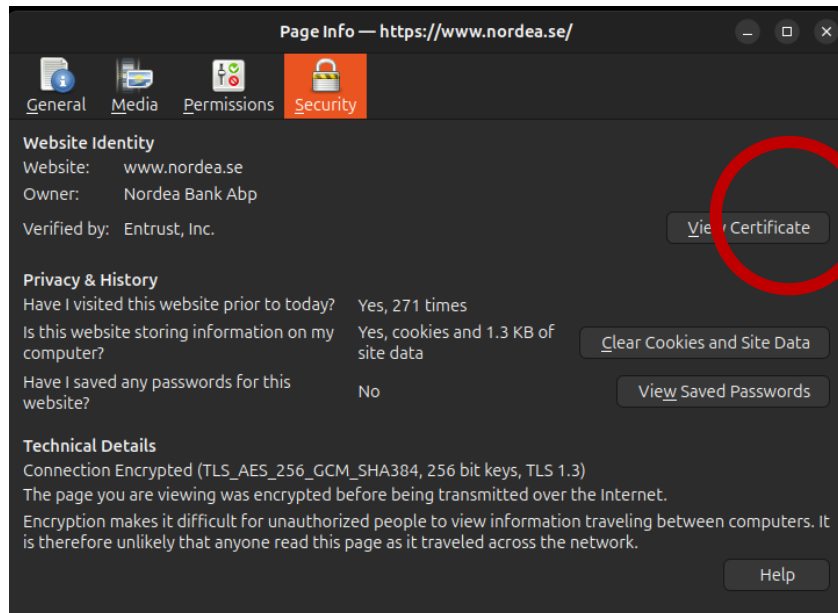
How to prove it ?

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

Authentication



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



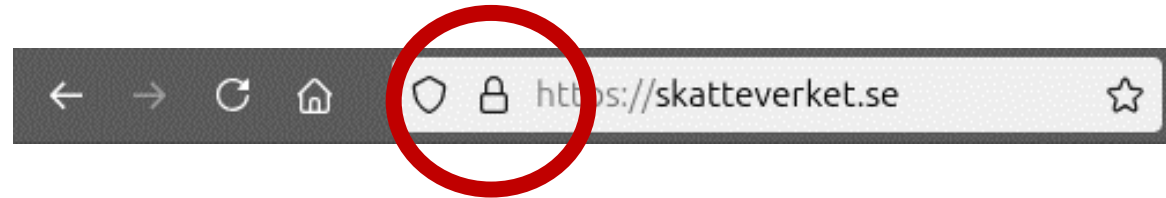
a signed public key
issued by the signer



It requires a lot of infrastructure around it ➡ PKI

Certificates and Certificates Authorities

Trust me!

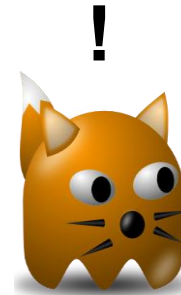
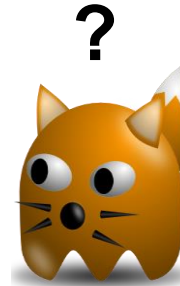


Certificate

skatteverket.se DigiCert EV RSA CA G2 DigiCert Global Root G2

Subject Name	
Inc. Country	SE
Business Category	Government Entity
Serial Number	Government Entity
Country	SE
State/Province	Stockholms län
Locality	Sundbyberg
Organization	Skatteverket
Common Name	skatteverket.se

Issuer Name	
Country	US
Organization	DigiCert Inc
Common Name	DigiCert EV RSA CA G2



Certificate Manager

Your Certificates Authentication Decisions People Servers **Authorities**

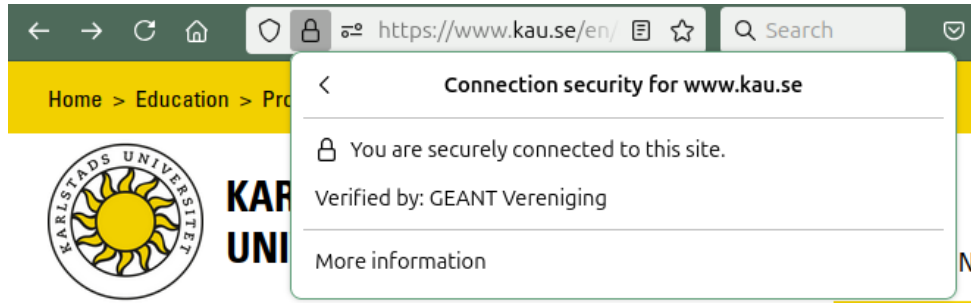
You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
> D-Trust GmbH	
> Deutsche Telekom Security GmbH	
> Dhimyotis	
> DigiCert Inc	
DigiCert Assured ID Root CA	Builtin Object Token
DigiCert Trusted Root G4	Builtin Object Token
DigiCert Global Root CA	Builtin Object Token
DigiCert Assured ID Root G3	Builtin Object Token
DigiCert High Assurance EV Root CA	Builtin Object Token
DigiCert Global Root G2	Builtin Object Token
DigiCert Assured ID Root G2	Builtin Object Token
DigiCert Global Root G3	Builtin Object Token
> DigiCert, Inc.	
> Digital Signature Trust Co.	
> DigitalSign Certificadora Digital	
> Disig a.s.	
> e-commerce monitoring GmbH	
> E-Tuğra EBG Bilişim Teknolojileri ve Hiz...	

View... Edit Trust... **Import...** Export... Delete or Distrust...

OK

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

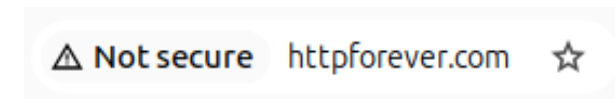
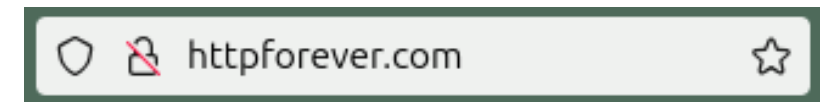
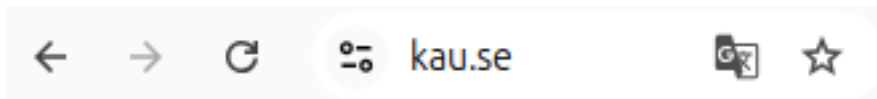
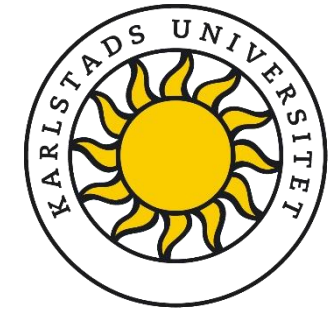
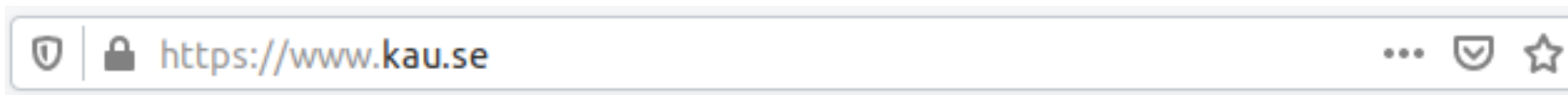
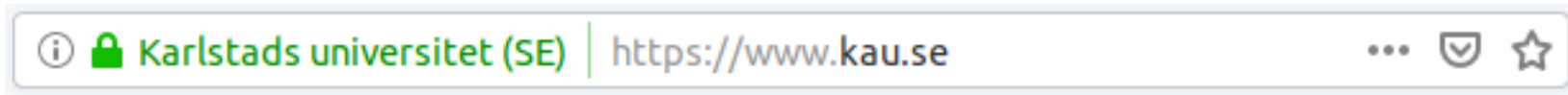
Policy	ANSI Organizational Identifier (2.16.840)
Value	2.16.840.1.114412.2.1
Policy	Certificate Type (2.23.140.1.1)
Value	Extended Validation
Qualifier	Practices Statement (1.3.6.1.5.5.7.2.1)
Value	http://www.digicert.com/CPS

Authentication

- Is this good authentication?



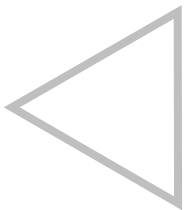
What about these?



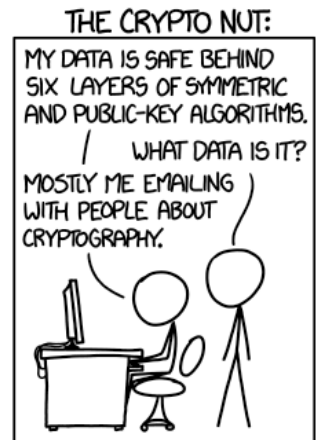
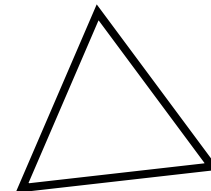
Computer and Network Security

Objectives:


- Confidentiality
- Integrity
- Availability

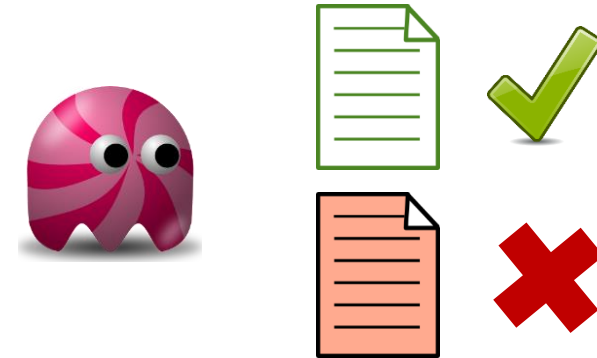
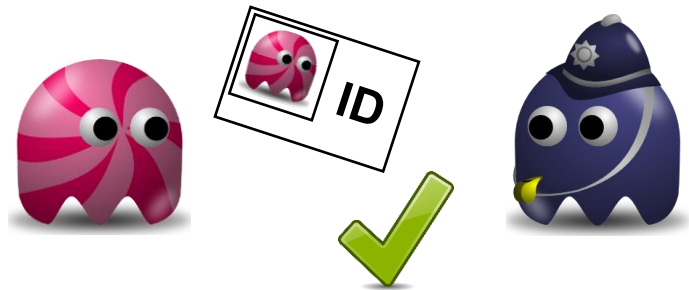


- Authentication
- ↓
- Authorization
 - Accounting

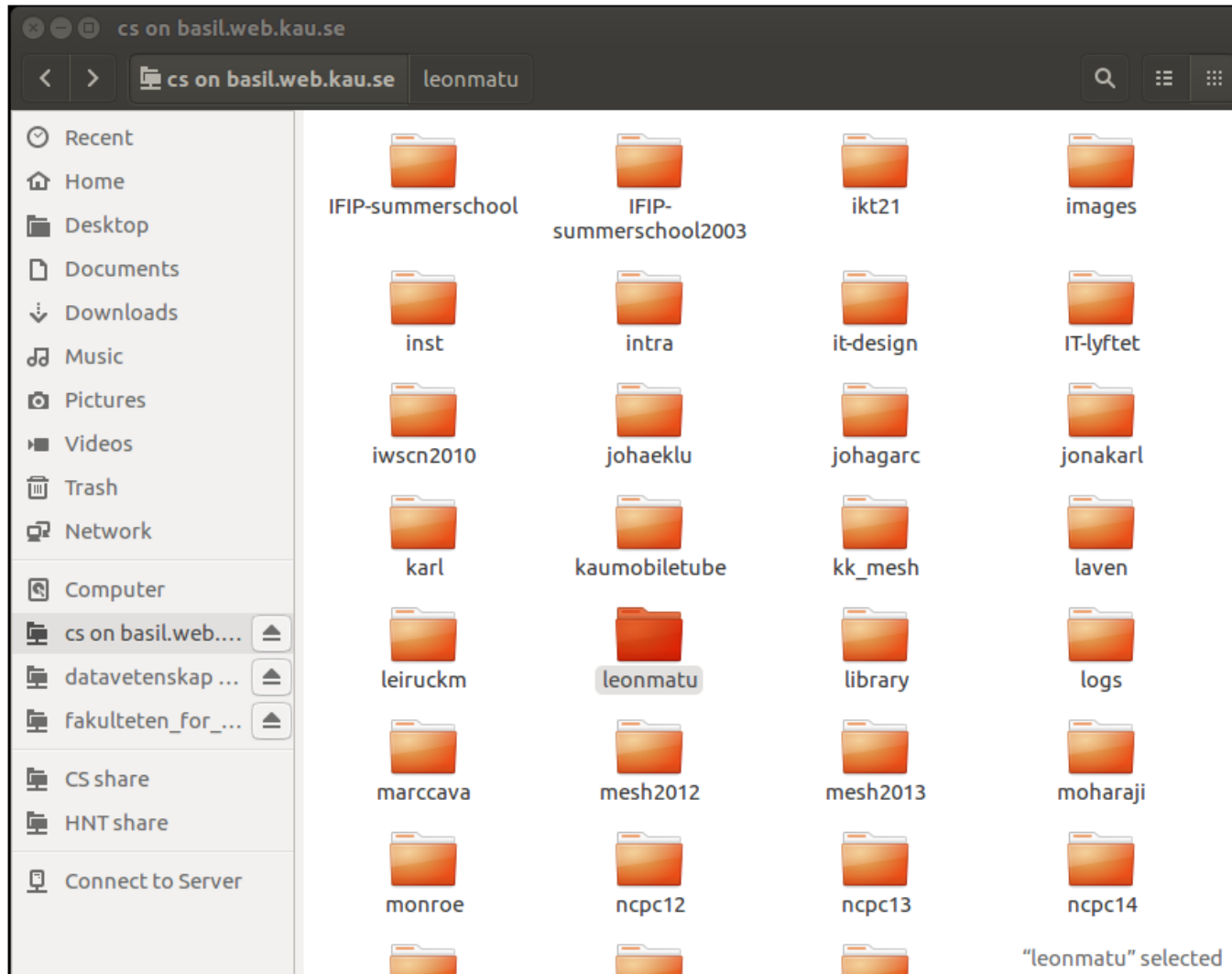


Authorization

- 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



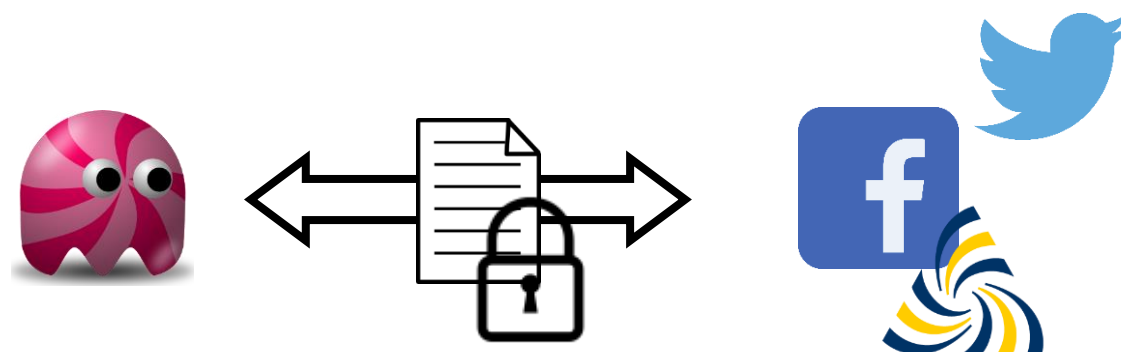
+ Symmetric and Asymmetric keys

+ Hash functions



+ Examples

It's Everywhere



🛡️ 🔒 🔗 <https://www.kau.se> ★

🛡️ 🔒 <https://skatteverket.se> ★

🛡️ 🔒 🔗 <https://www.nordea.se> ★

Next

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

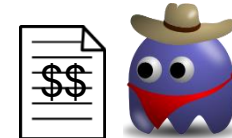
Q3. In the following scenarios, explain what type of security violations are present (if any).


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.