

Security Fundamentals

DVGC19



KARLSTAD
UNIVERSITY
SWEDEN

Leonardo A. Martucci

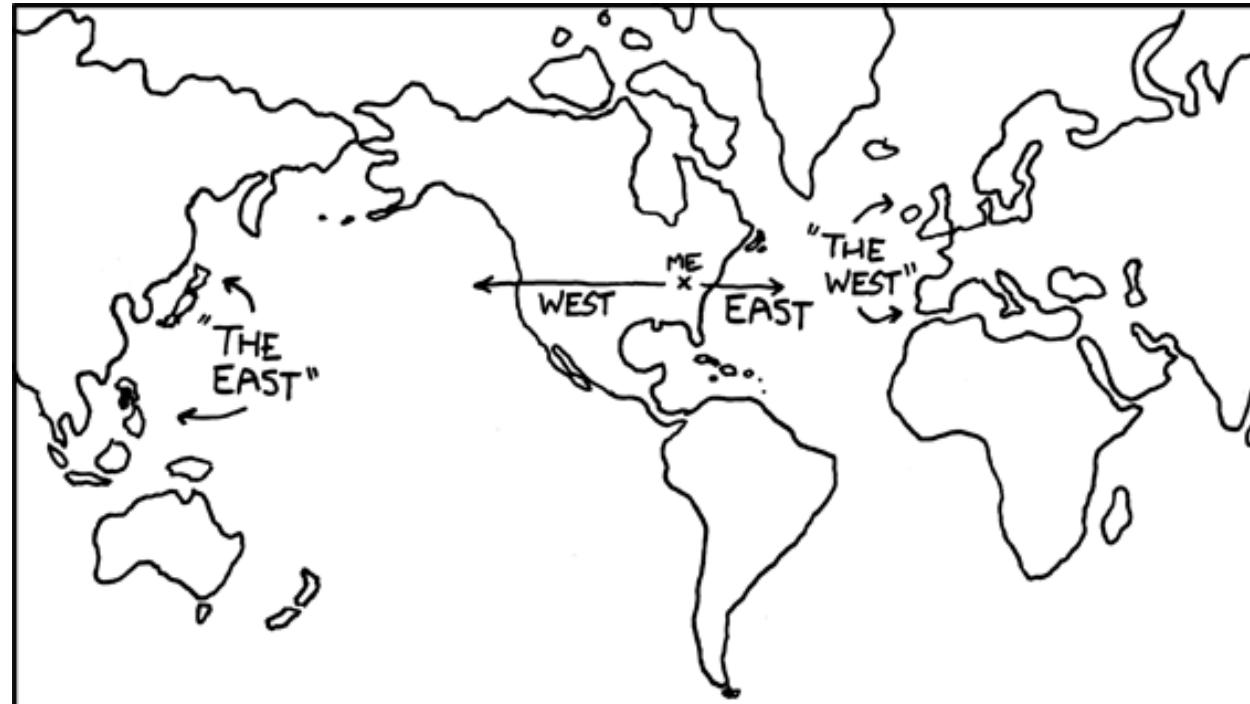
Lectures

- 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



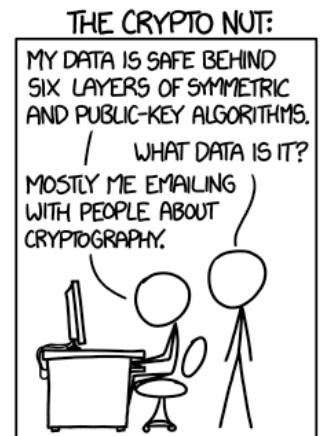
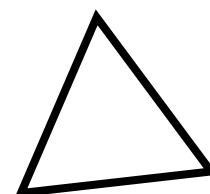
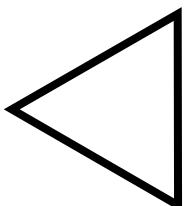
OPINIONS ON INTERNET PRIVACY



Computer and Network Security

Objectives:

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



The Actors

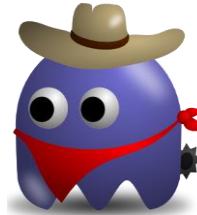
- Alice



- Eve (Mallory)



- Bob



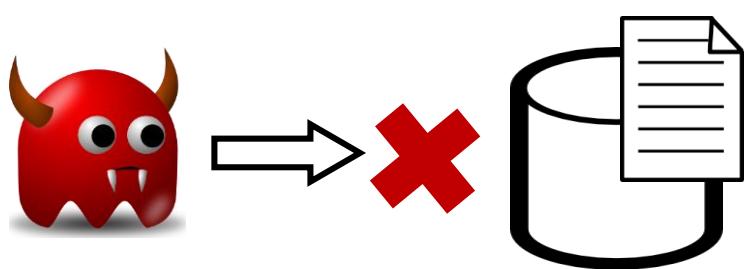
(+ The Support Cast)



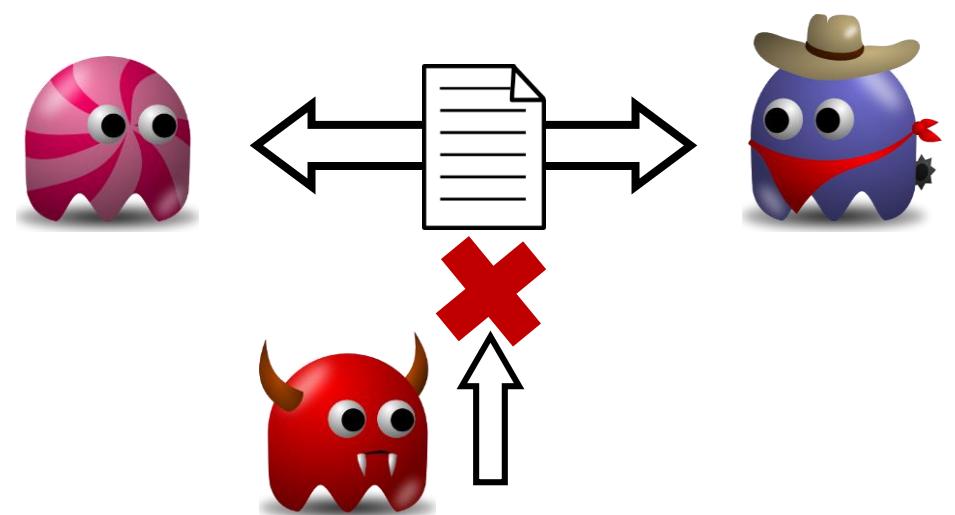
Confidentiality

- Information NOT available or disclosed to unauthorized parties

- Stored Data



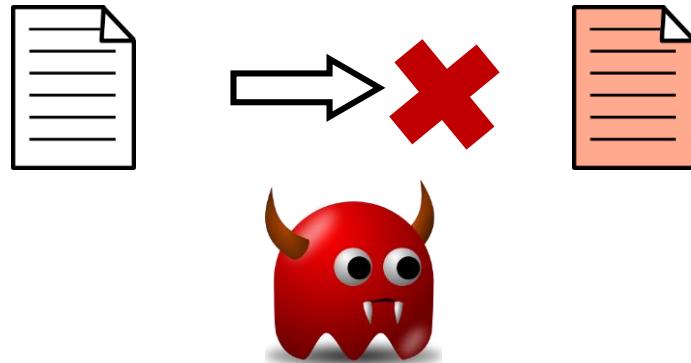
- Data in Transit



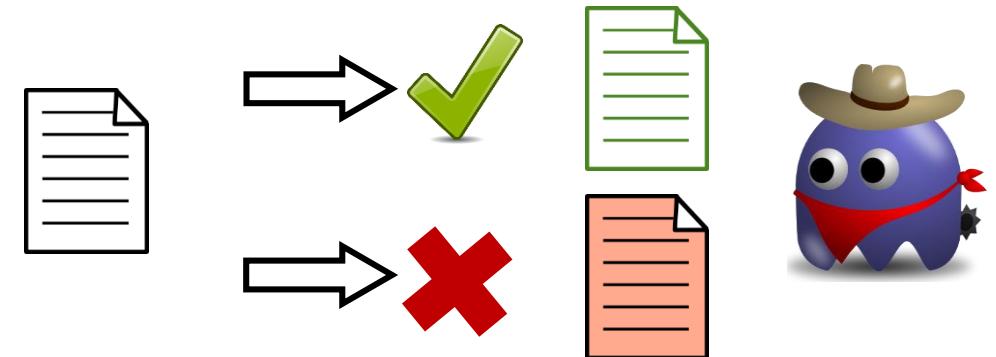
Integrity

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

- Unauthorized Parties

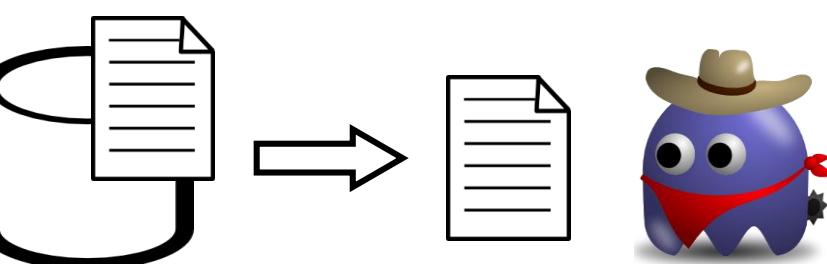


- Unauthorized Manner



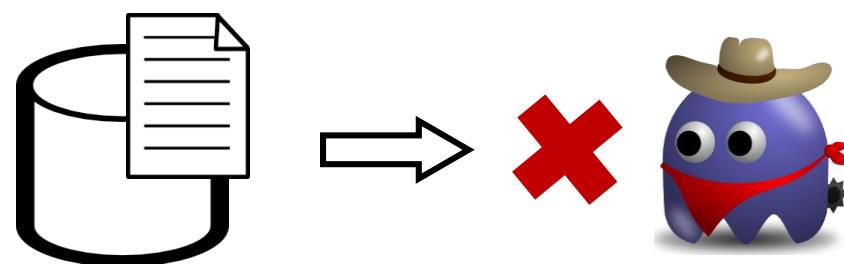
Availability

- Information available when needed



- Available

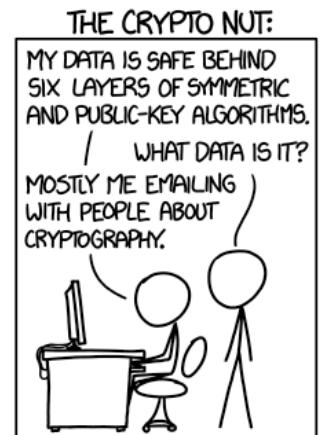
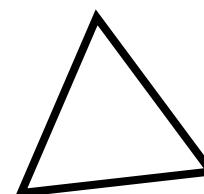
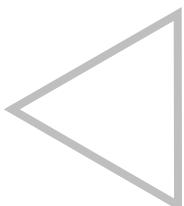
- NOT Available



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

The image shows a screenshot of a web browser window titled "Log In to Canvas - Opera". The address bar shows "pbd.cs.kau.se/login/canvas". A "Secure connection" message is displayed, stating "pbd.cs.kau.se The connection is secure." Below this is a "Details" link. The main content area shows a login form for "Open Source LMS INSTRUCTURE". The form includes fields for "Email" and "Password", a "Stay signed in" checkbox, and links for "Forgot Password?" and "Log In". At the bottom of the form, the text "Open Source LMS INSTRUCTURE" is visible. To the right of the main window, a separate "Certificate Viewer" window is open, showing detailed information about the SSL certificate for pbd.cs.kau.se. The "General" tab is selected, displaying the common name as "pbd.cs.kau.se", the organization as "<Not Part Of Certificate>", and the issuer as "Let's Encrypt Authority X3". The "Validity Period" tab shows the certificate was issued on Wednesday, November 1, 2017 at 3:22:19 PM and expires on Tuesday, January 30, 2018 at 3:22:19 PM. The "Fingerprints" tab lists SHA-256 and SHA-1 fingerprints.

Common Name (CN)	Let's Encrypt Authority X3
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued On	Wednesday, November 1, 2017 at 3:22:19 PM
Expires On	Tuesday, January 30, 2018 at 3:22:19 PM

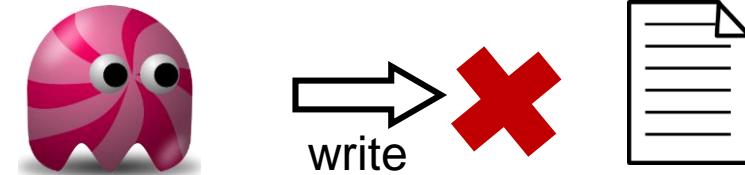
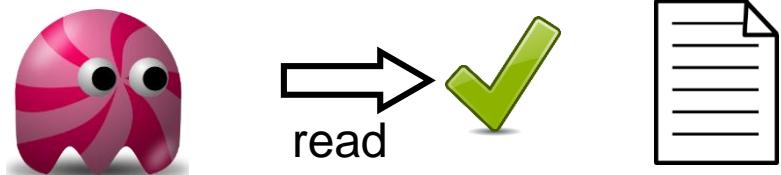
SHA-256 Fingerprint	SHA-1 Fingerprint
CD 30 67 80 18 5D 1F 61 AC 8C BD 6A CC EE 8C 6C B3 0C 07 F3 97 C1 94 68 SF 32 65 AF 39 3F 2B 8A A2 DA EE 35 YA BB B9 CC F5 77 93 TD 53 26 SD 83 84 0A 66 F0	

Authorization

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

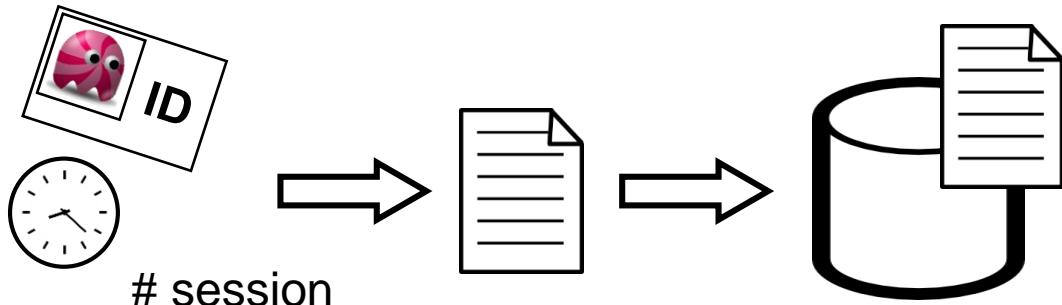


- Authorized
- NOT Authorized



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

hash () 



= message (arbitrary)
= digest (fixed length)

meaning:

 f () 

+ a number of security properties (C20!)

Building Blocks

- message



- cyphertext



- encryption function $\rightarrow e()$

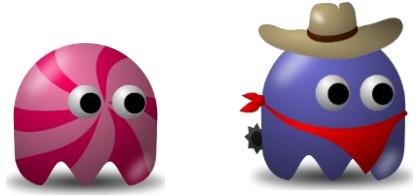
- decryption function $\rightarrow d()$

- key(s)

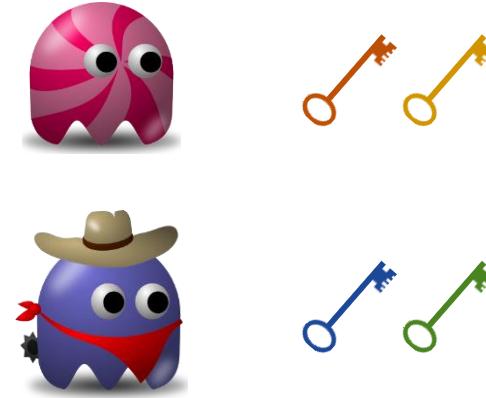


Algorithms and Keys

symmetric



asymmetric

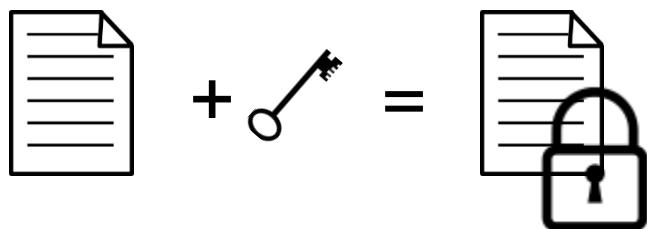
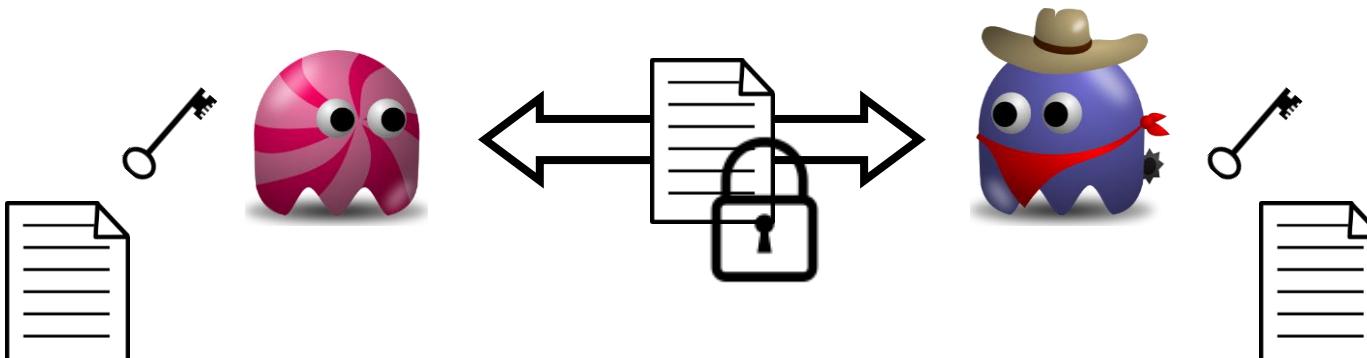


- 1 (shared) key

- 2 key pairs

Symmetric Encryption

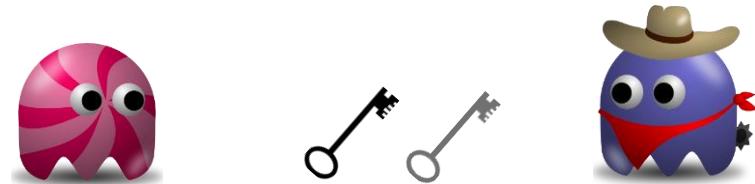
- Alice & Bob → 1 shared key



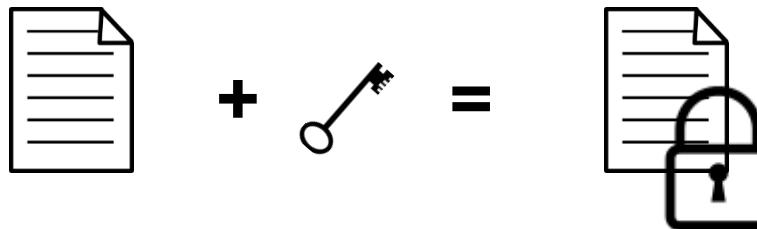
there many ways on how to do (e, d)

Symmetric Encryption in Practice

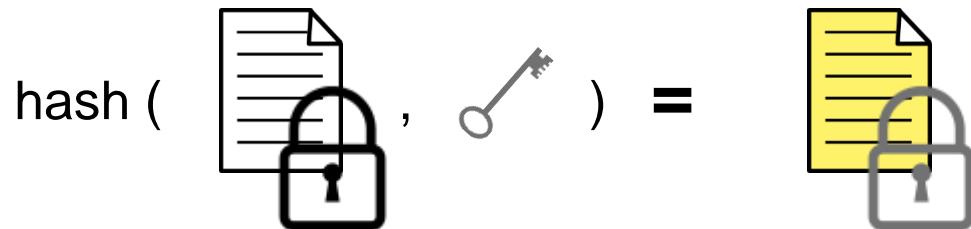
- with symmetric keys:
authenticated encryption (EtM)



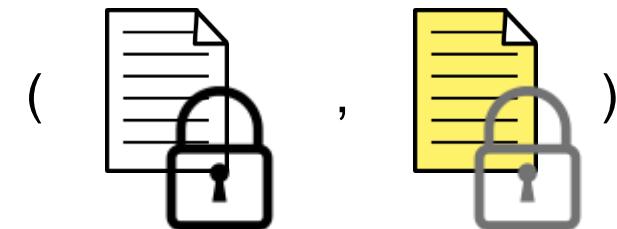
2 shared keys



encrypt-then-MAC message

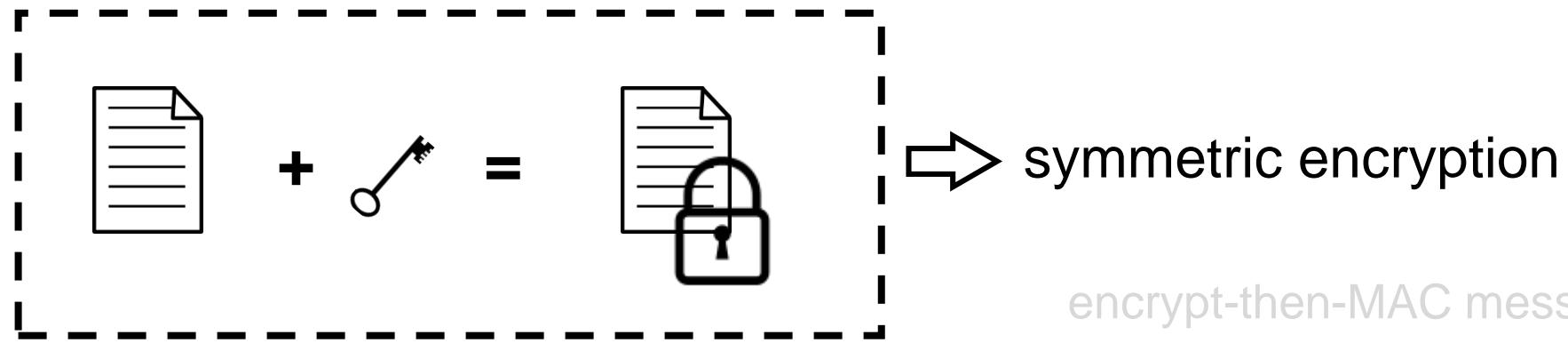
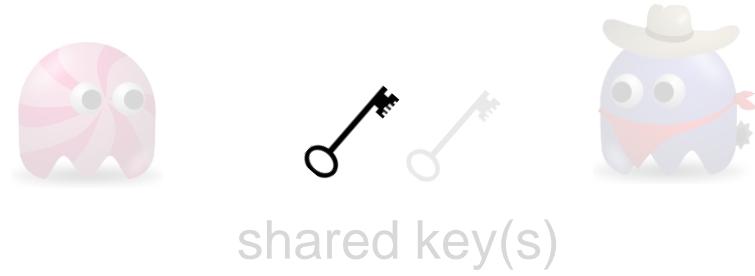


* keyed hash



Symmetric Encryption in Practice

- with symmetric keys:
authenticated encryption (EtM)



encrypt-then-MAC message

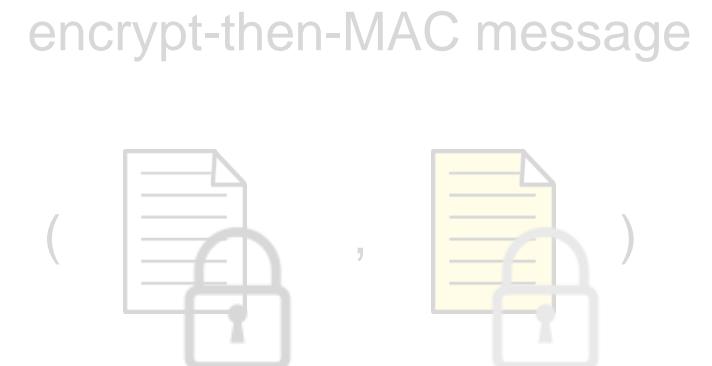
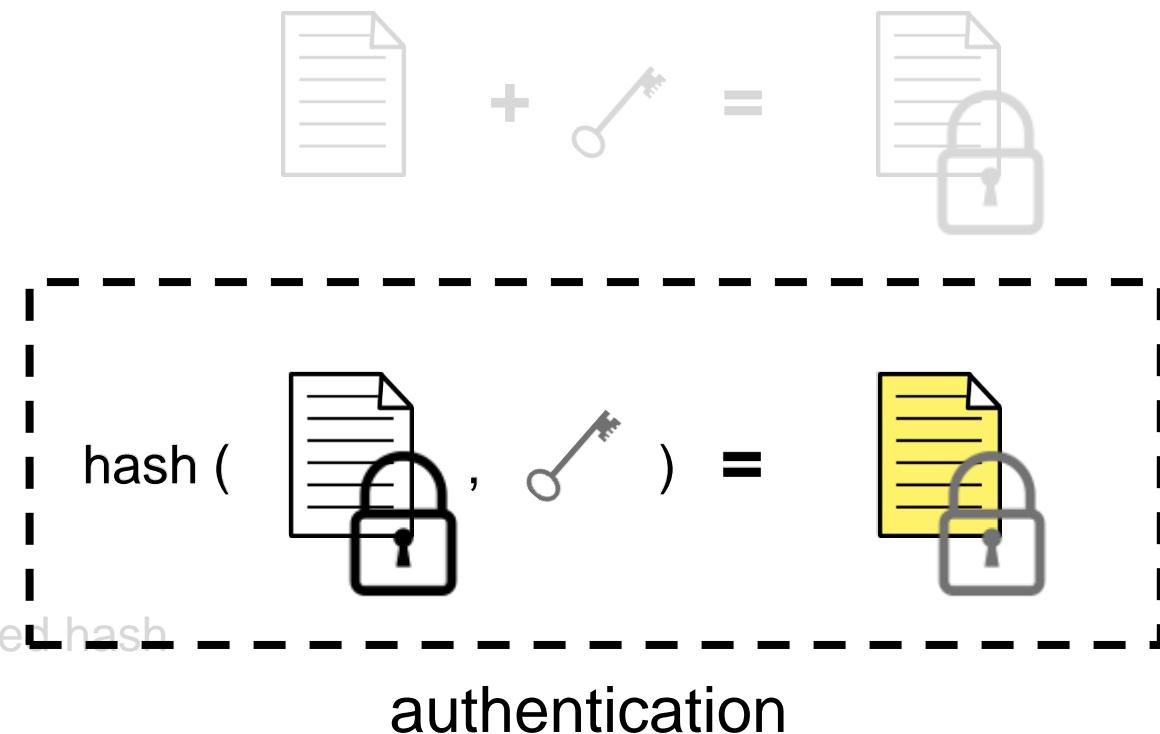
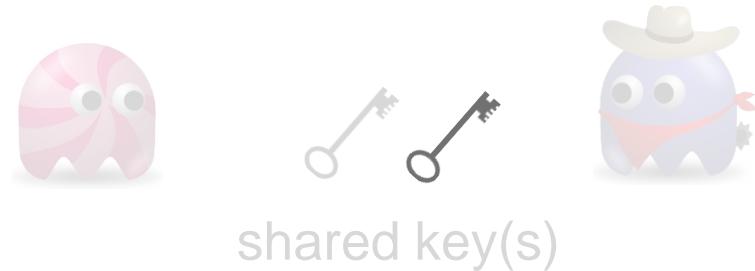


* keyed hash



Symmetric Encryption in Practice

- with symmetric keys:
authenticated encryption (EtM)



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)



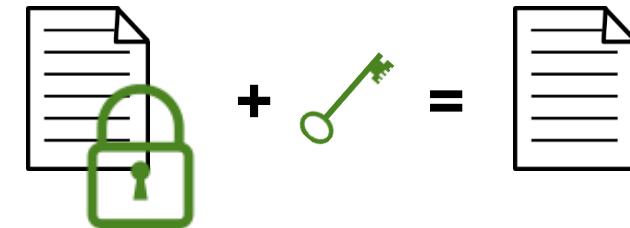
encrypts with



public key

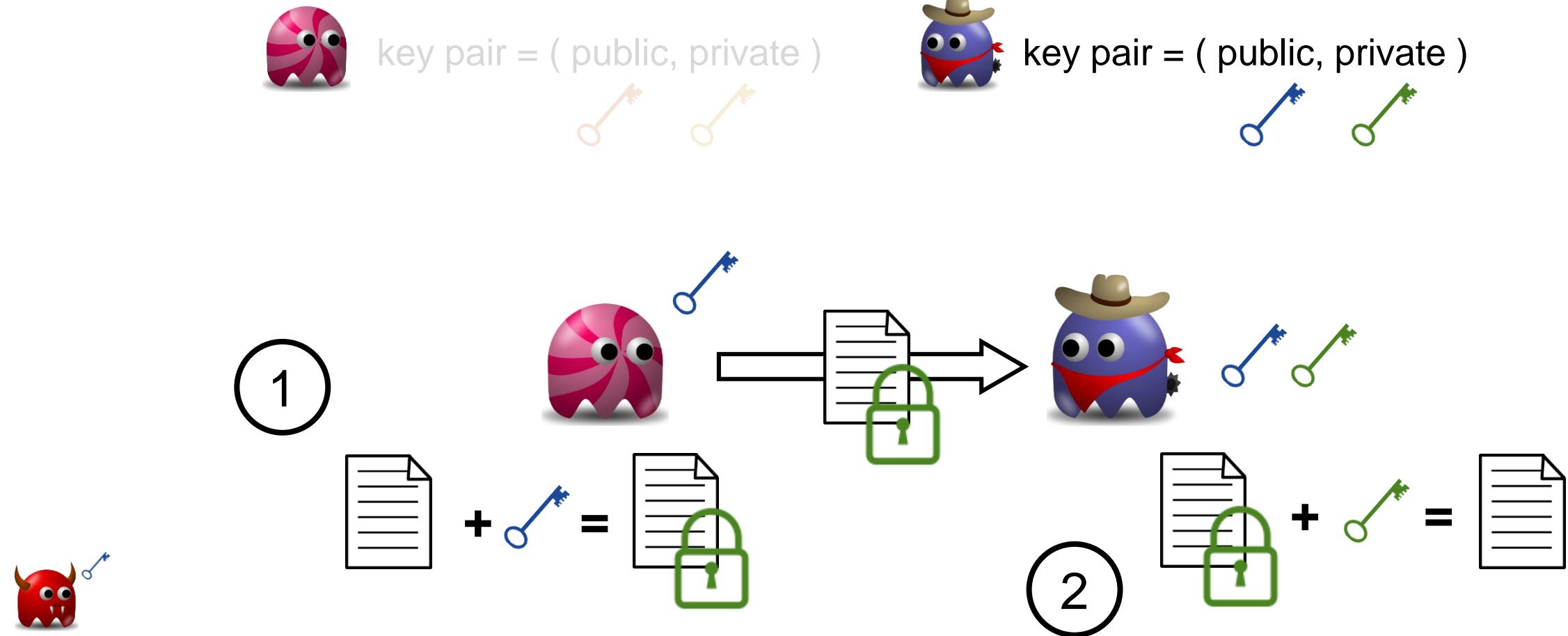


decrypts with his private key



Asymmetric Encryption: Confidentiality

- Alice sends a message to Bob



Asymmetric Encryption: Confidentiality

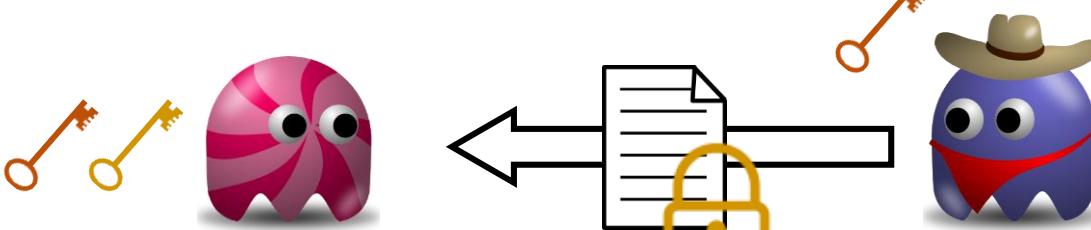
and Bob responds



key pair = (public, private)



key pair = (public, private)



1

2

A diagram showing a document with a yellow padlock on it. A key is shown next to it. An equals sign follows, and another document without a lock is shown to the right.
$$\text{locked document} + \text{key} = \text{unlocked document}$$

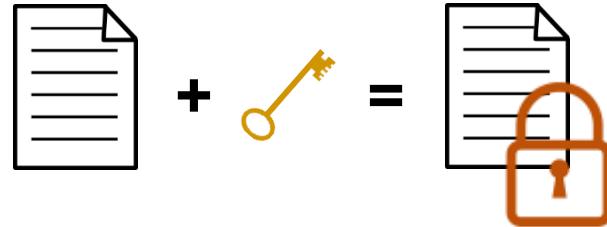
A diagram showing a document with a yellow padlock on it. A key is shown next to it. An equals sign follows, and another document with a yellow padlock on it is shown to the right.
$$\text{locked document} + \text{key} = \text{locked document}$$

Asymmetric Encryption: Authentication

- Can be used to authenticate (sign)



key pair = (public, private)



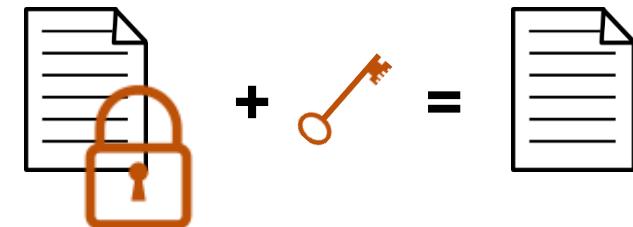
signs with her private key



key pair = (public, private)

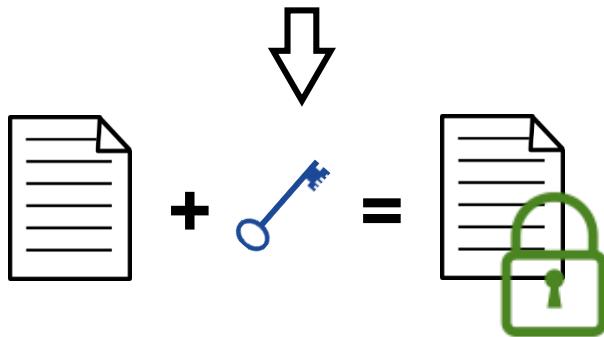


verifies with public key

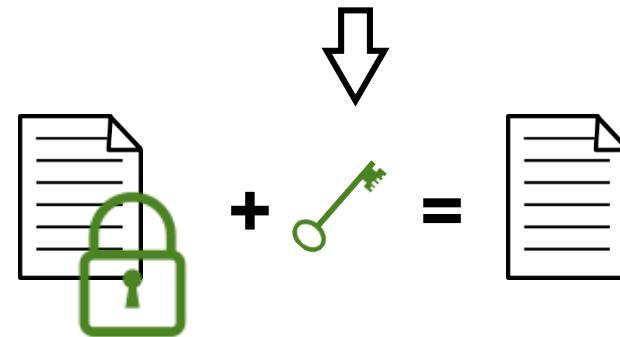


Asymmetric Encryption Cheat Sheet

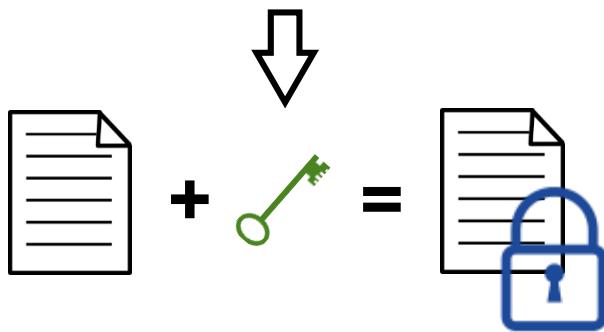
- Encrypts with Public Key



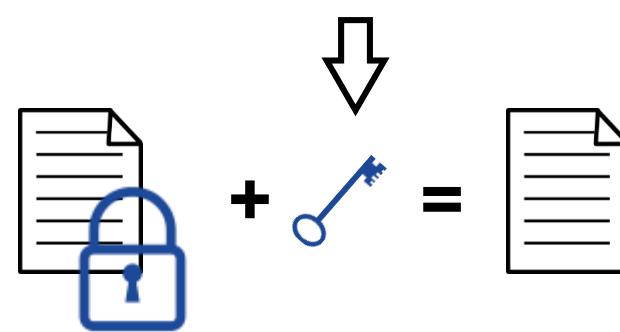
- Decrypts with Private Key



- Signs with Private Key

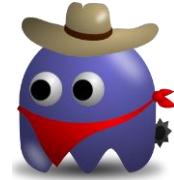


- Verifies with Public Key



Symmetric + Asymmetric in Practice

- public key encryption + symmetric key encryption + hashing



private key
public key

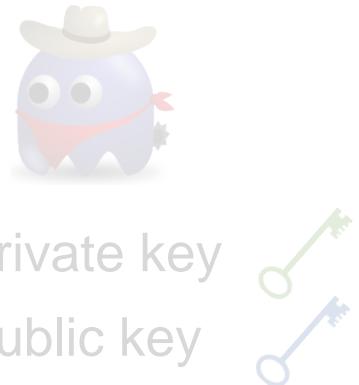
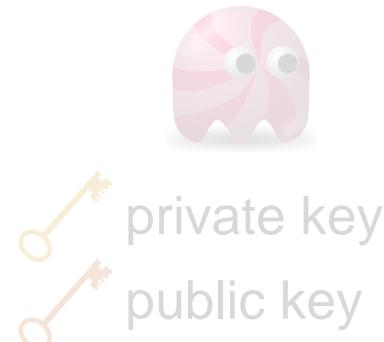
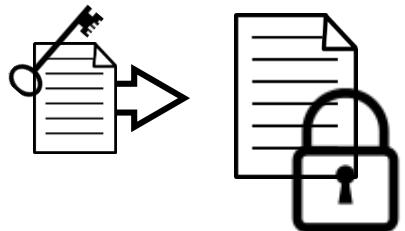


Symmetric + Asymmetric (PGP)

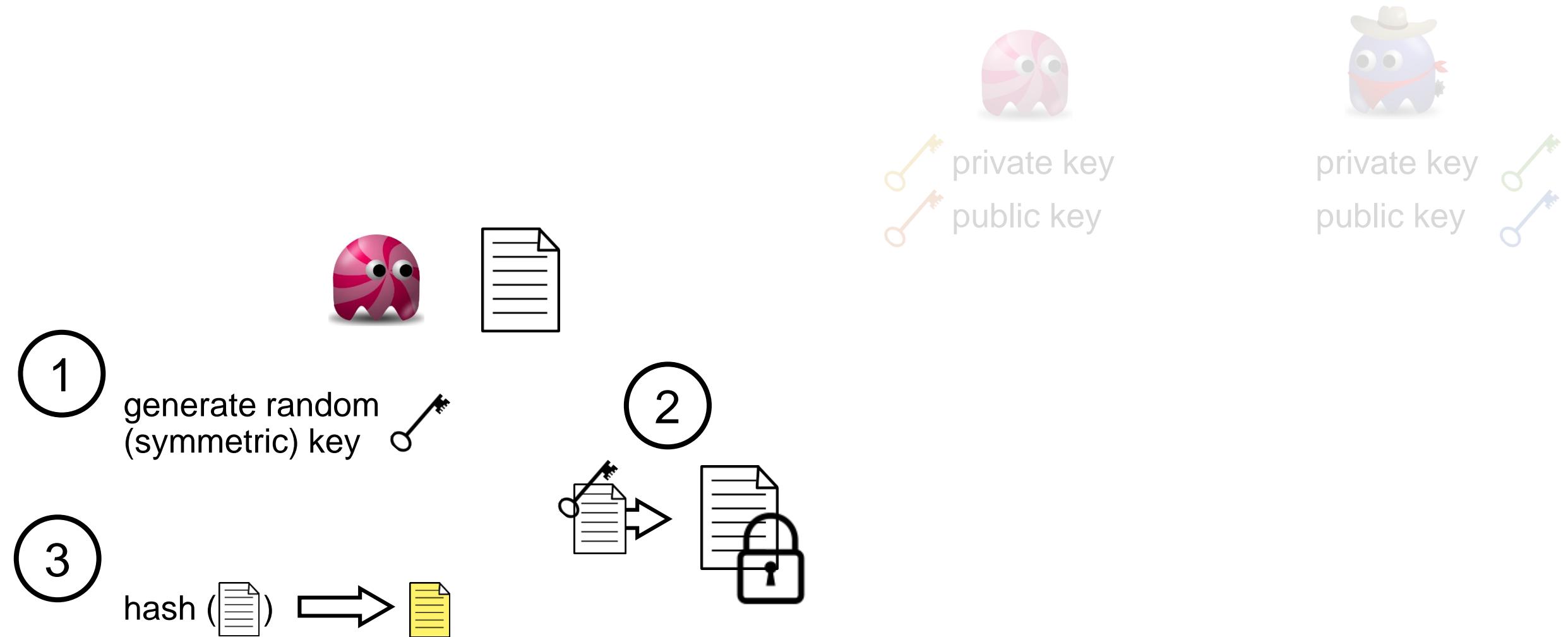
- public key and symmetric key encryption
+ hashing

1

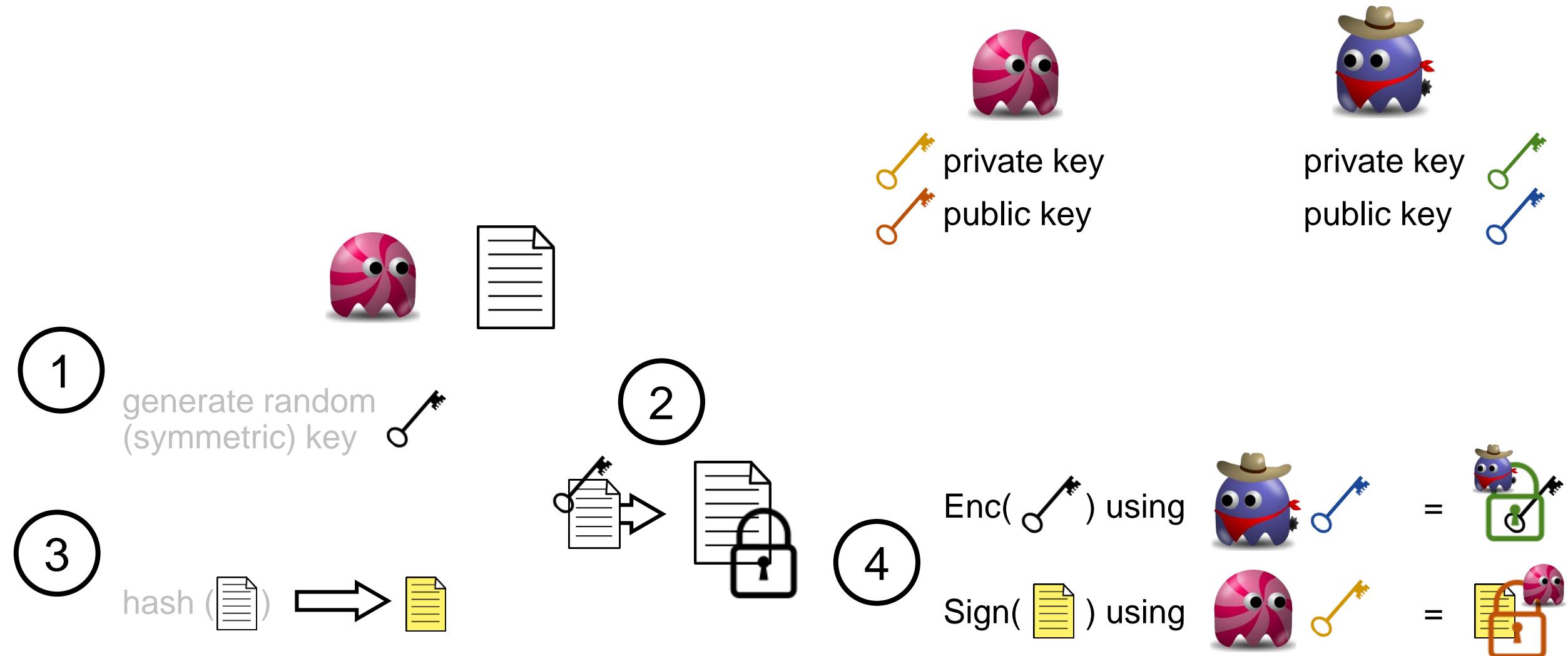
generate random
(symmetric) key



In practice (with PGP)

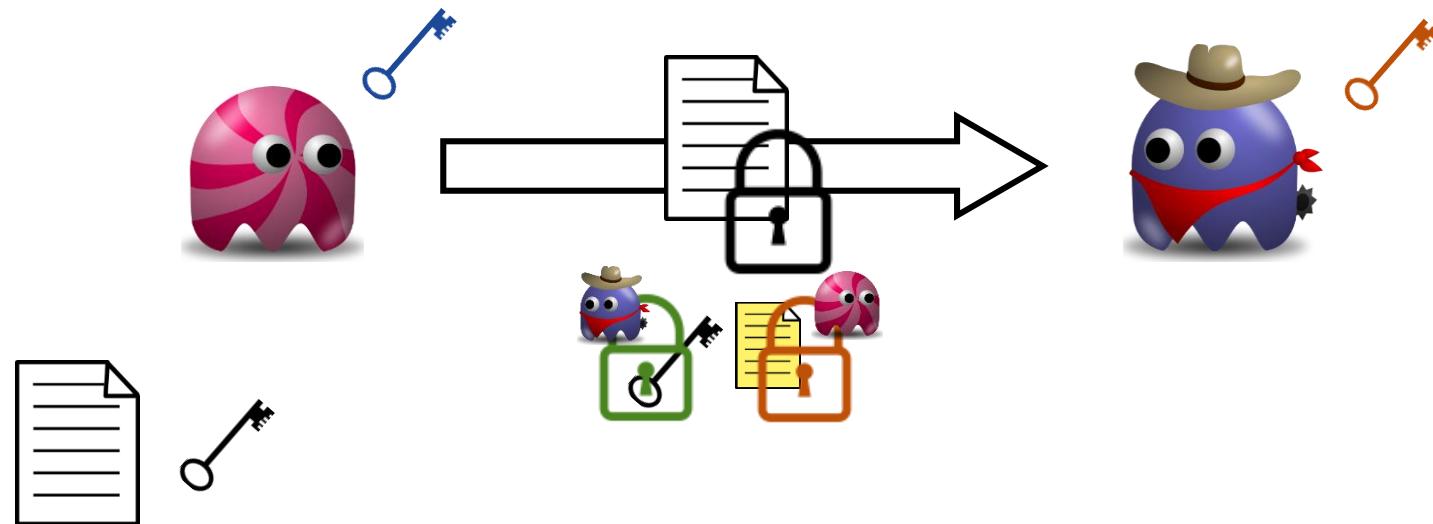
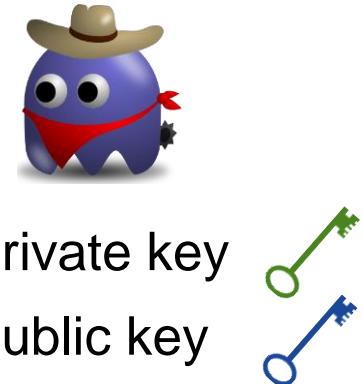


In practice (with PGP)



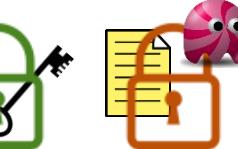
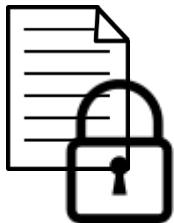
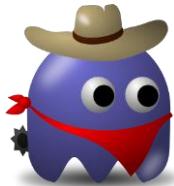
In practice (with PGP)

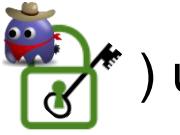
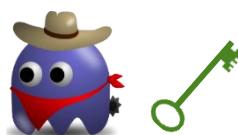
- Alice sends  and  to Bob



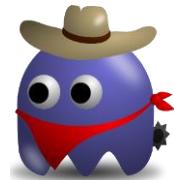
In practice (with PGP)

- public key and symmetric key encryption
+ hashing



- Dec() using  = 

- Dec() using  = 

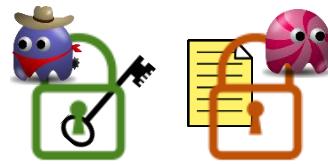
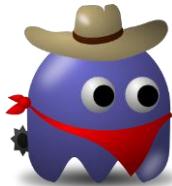


private key
public key



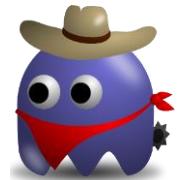
In practice (with PGP)

- public key and symmetric key encryption
+ hashing



• $\text{Dec}(\text{Encrypted File})$ using  = 

• $\text{Dec}(\text{Hashed File})$ using  = 



private key
public key

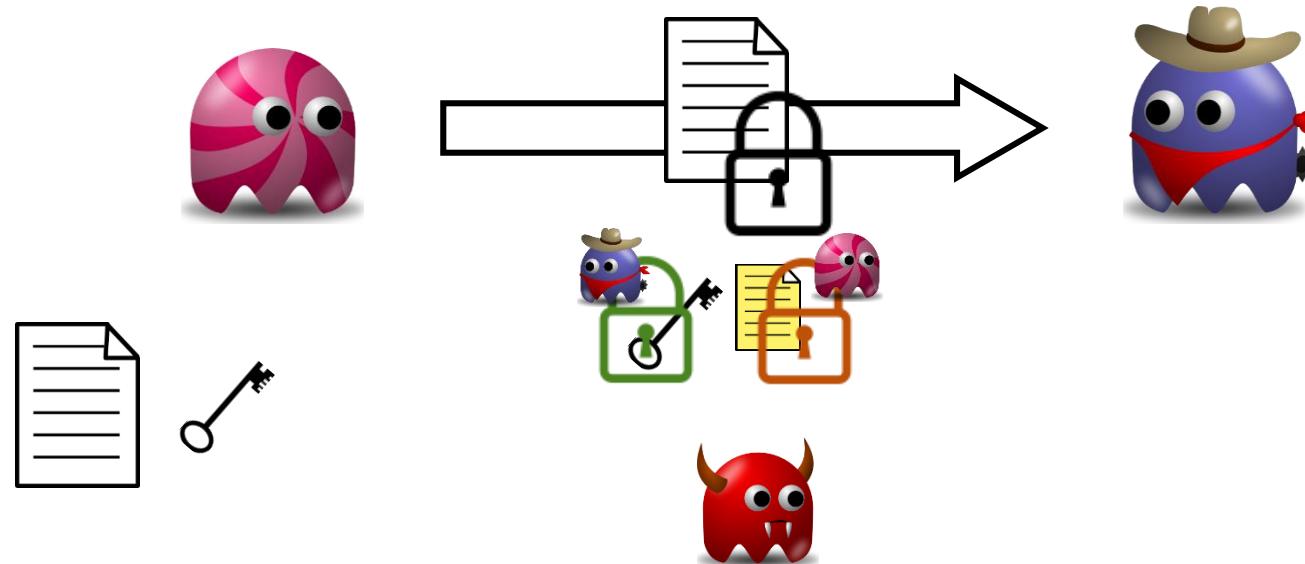
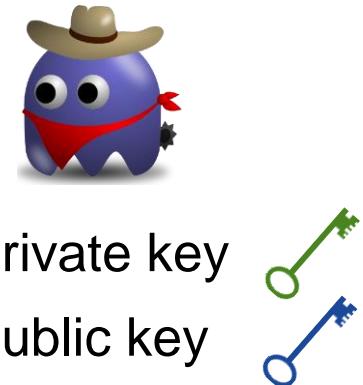


• $\text{hash}(\text{Document}) \rightarrow \text{Hash} \rightarrow \text{equal?}(\text{Hash}, \text{Hash})$ 

• $\text{Ver}(\text{Hashed File})$ using  and  = 

In practice (with PGP)

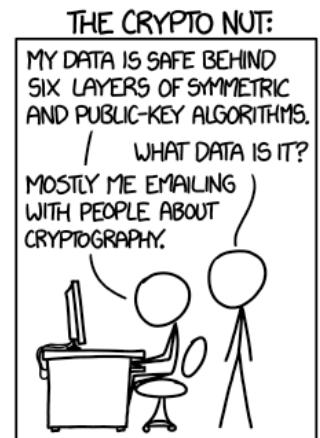
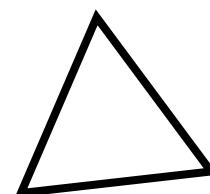
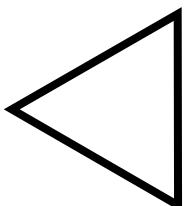
- public key and symmetric key encryption
+ hashing



Computer and Network Security

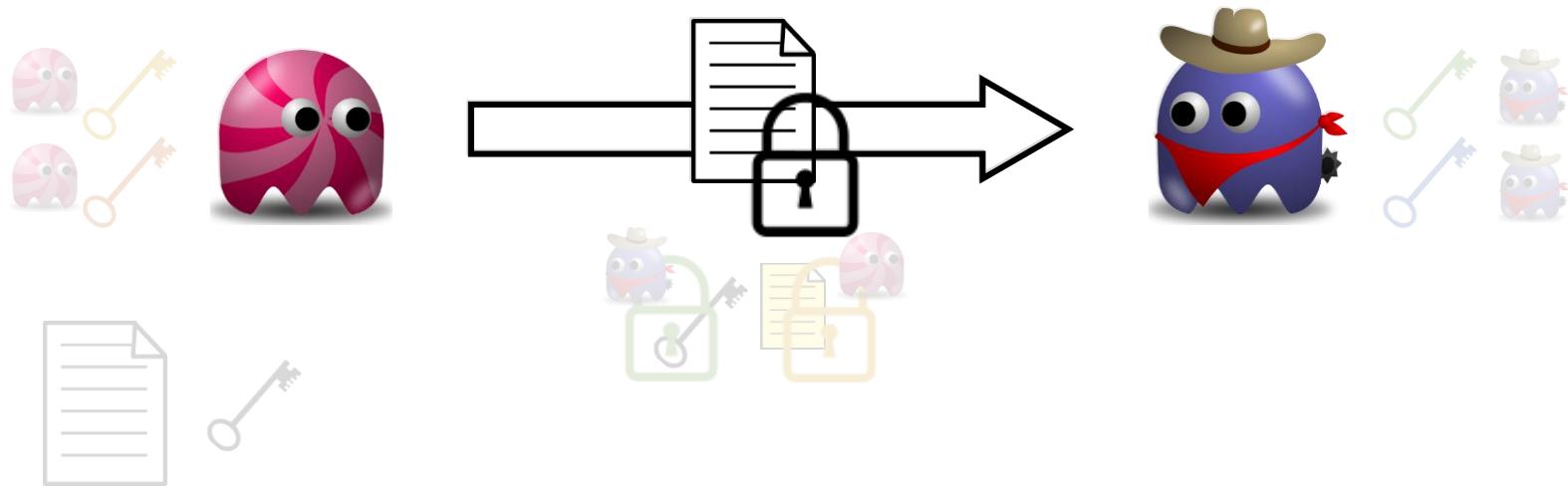
Objectives:

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



Confidentiality

- public key and symmetric key encryption
+ hashing



private key
public key

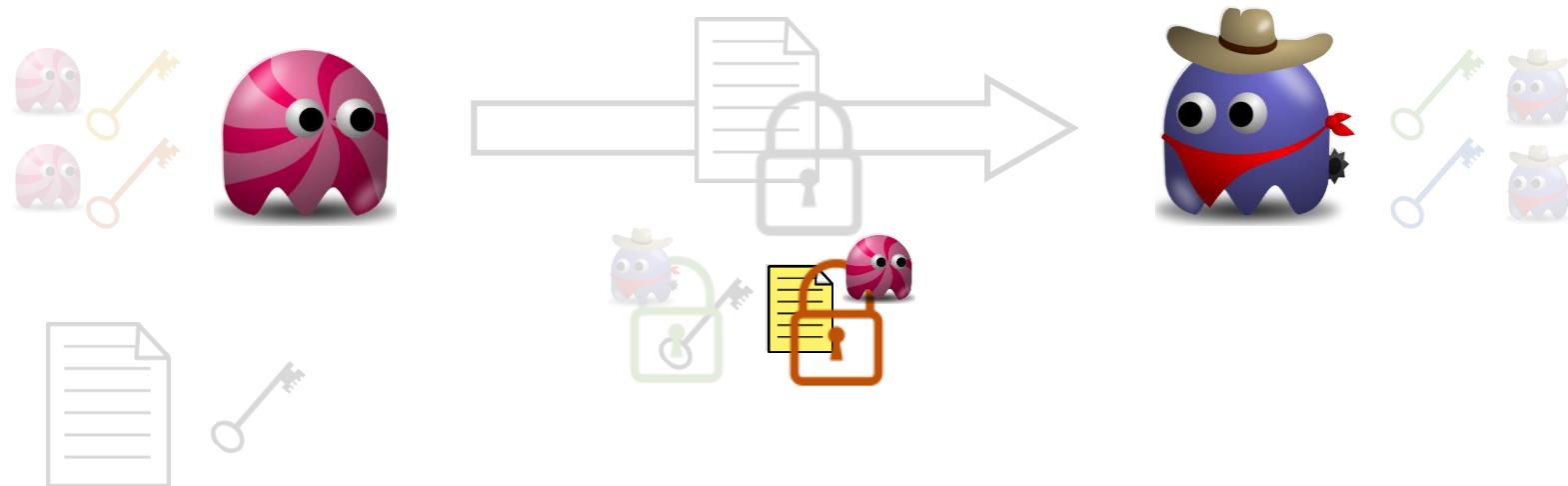


private key
public key



Integrity

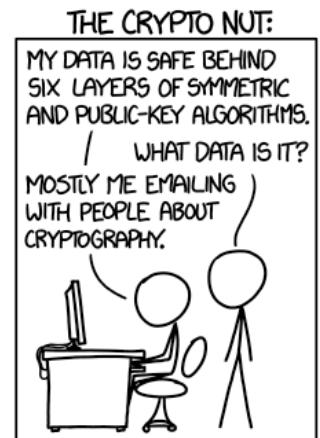
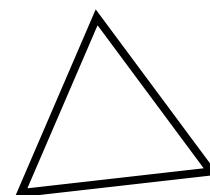
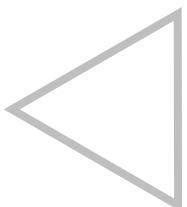
- public key and symmetric key encryption
+ hashing



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

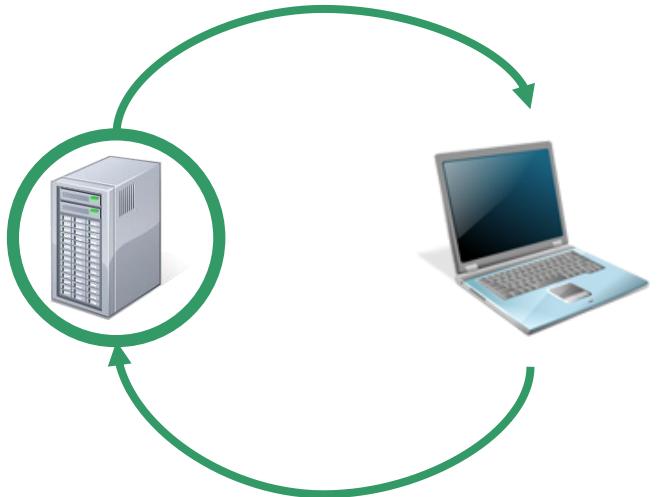
Are you really who you claim to be?



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

Page Info — https://www.nordea.se

General Media Permissions Security

Website Identity

Website: www.nordea.se
Owner: Nordea Bank Abp
Verified by: Entrust, Inc.

Privacy & History

Have I visited this website prior to today? Yes, 271 times
Is this website storing information on my computer? Yes, cookies and 1.3 KB of site data
Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_AES_256_GCM_SHA384, 256 bit keys, TLS 1.3)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

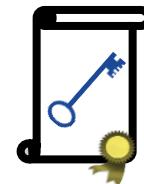
View Certificate

Clear Cookies and Site Data

View Saved Passwords

Help

a signed public key issued by the signer



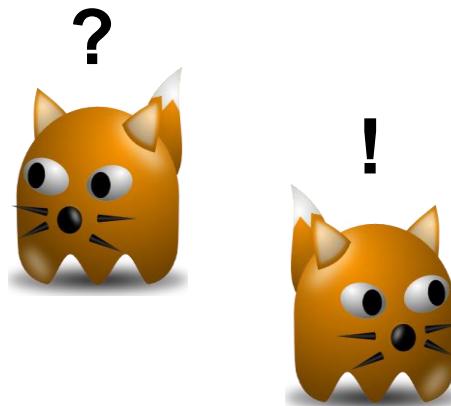
It requires a lot of infrastructure around it → PKI

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

The screenshot shows a web browser window with the URL <https://www.kau.se/en/>. A certificate information dialog is open, stating "You are securely connected to this site. Verified by: GEANT Vereniging". Below the browser is a table titled "Certificate Policies" with two entries:

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?



ⓘ 🔒 Karlstads universitet (SE) | <https://www.kau.se> ... 🌐 ⭐

ⓘ 🔒 <https://www.kau.se> ... 🌐 ⭐

ⓘ 🔒 ↻ <https://www.kau.se> ⭐



⏪ ⏩ ⏴ ↻ kau.se 🌐 ⭐

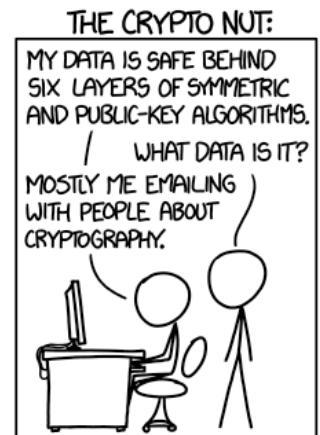
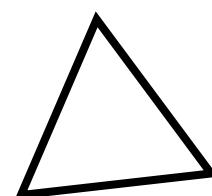
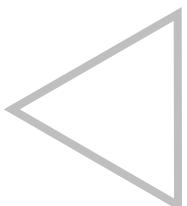
ⓘ 🔒 <http://httpforever.com> ⭐

⚠ Not secure <http://httpforever.com> ⭐

Computer and Network Security

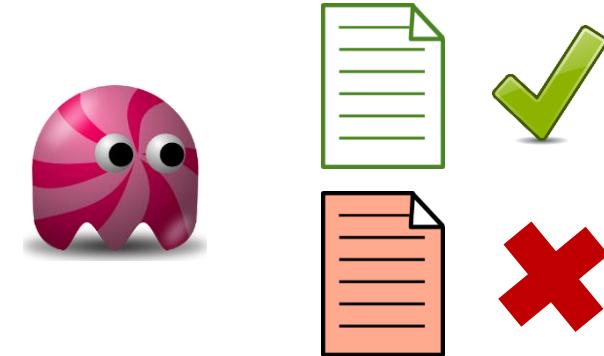
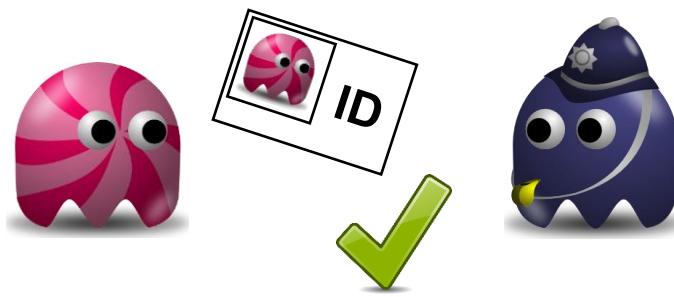
Objectives:

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

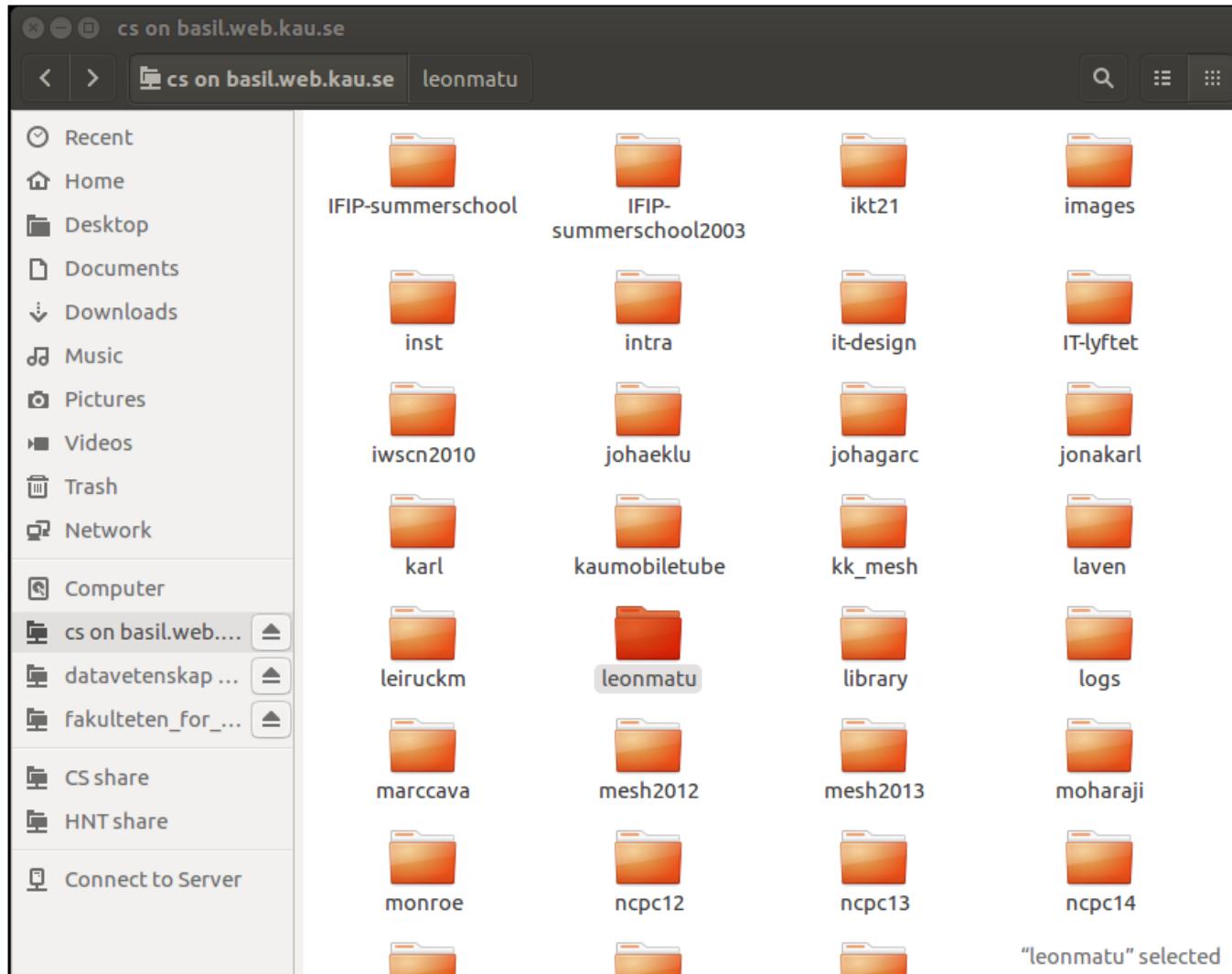


Authorization

- 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

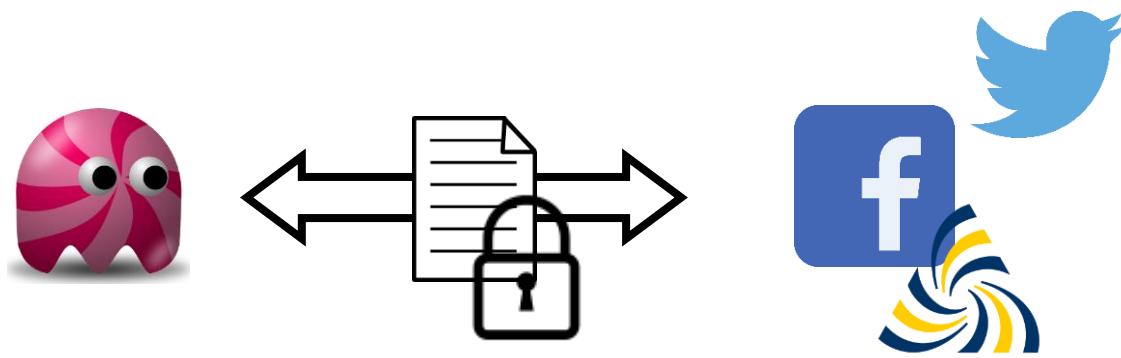


- + Symmetric and Asymmetric keys
- + Hash functions



- + Examples

It's Everywhere



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?
- c. computational performance?
- d. key distribution?

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