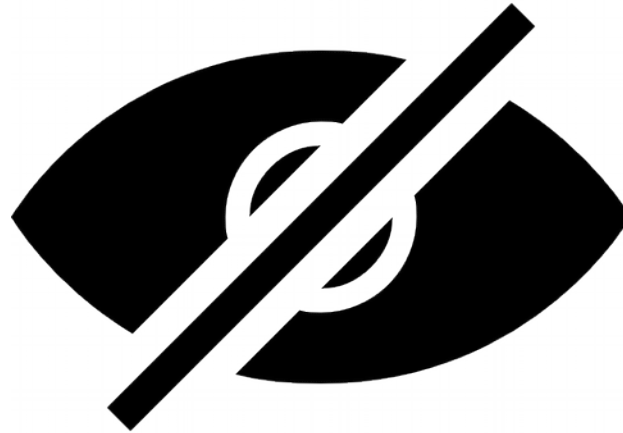


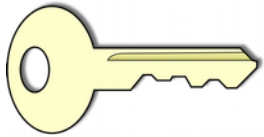
# Basic cryptography



BUITA lecture 8  
Thursday October 4th, 2018

Niels Jorgensen  
(nielsj@ruc.dk)

# Agenda today



1. Introduction to security with a focus on encryption

2. Symmetric encryption

3. Asymmetric encryption



*“Basic cryptography”*


4. Exercise: PIA of your project => encryption?

5. Introduction to next time: *“Applied cryptography”*

# Learnings goals - “basic cryptography”

## Today

- Know about basic cryptography, including symmetric and asymmetric encryption.
- Be able to choose and use among basic cryptographic techniques and build secure solutions by utilizing them

 sketch, discuss

## PIA exercise

- identify valuable/threatened data in your project
- protective measures - encryption?

## Next time - “applied cryptography”

- passwords, digital signatures
- mainly as used in secure login

# The Information Commissioner's Office: *Encryption*

*“The two main purposes for which [we] may consider using encryption are data storage and data transfer.” (p 5)*

Exercise:

For each purpose, what is encryption useful for?  
(According to the article.)

# The Information Commissioner's Office: *Encryption*

*“The two main purposes for which [we] may consider using encryption are data storage and data transfer. “ (p 5)*

Exercise:

For each purpose, what is encryption useful for?  
(According to the article.)

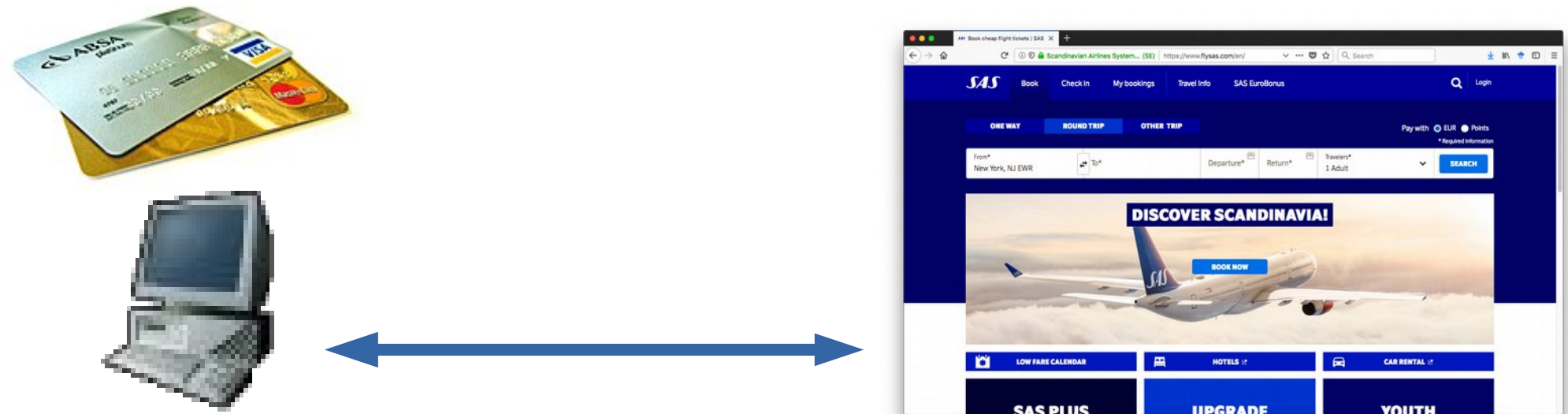
*Data storage:*

- *“unauthorized or unlawful processing” (of the stored data)*
- *“especially .. if data is lost or stolen”*
- *Police example (copying data)*

*Data transfer:*

- *“interception [...] by a third party whilst the data is in transfer”*

# Online payments



You are buying an airline ticket online, using a payment card

Data sent and stored include

- airline ticket (src, dest, date)
- price
- card#, account#, security#,...

*Exercise:*

- *is “encryption of stored data” relevant?*
- *is “encryption of transient data” relevant?*

# Answer

## *Encryption of stored data: Relevant*

- to protect your account data
  - eg. at Nets, the company that handles the Dankort payment card
- however, stored account data is typically not encrypted

## *Encryption of transmitted data: Relevant*

- your payment order contains card number + issue date + security code
- transmitted over the Internet or the mobile network
- encryption protects information from being read
- transmitted data of this sort is typically encrypted

# The scandal about “Se & Hør” (Watch and Listen)

The Danish weekly magazine “Se og Hør” brings stories & pictures about

- celebrities
- members of the royal family
- often intimate and private





# Prison sentences in 2016

The magazine's chief editor Henrik Quortrup was sentenced 1 year and 3 months of prison (though mostly suspended)

The “hush-hush” source Peter Bo Henriksen was sentenced 1 year and 6 months of prison

- had leaked information from Nets
- payments of hotels and airline tickets
- then the journalists would travel to the same hotels
- approx. 100 celebrities on watch-list
- the database was operated by IBM under an agreement with Nets

Apparently, IBM had no privacy measures in place

- *“It was normal to check how ex-lovers and celebrities were using their cards” (among people employed in Nets’ dept. of consumer service)*
- specific method unknown

- [da.wikipedia.org/wiki/Se\\_og\\_H%C3%B8r-sagen](https://da.wikipedia.org/wiki/Se_og_H%C3%B8r-sagen)
- [theguardian.com/world/2016/nov/24/two-convicted-of-tracking-credit-card-history-of-danish-royal-family](https://theguardian.com/world/2016/nov/24/two-convicted-of-tracking-credit-card-history-of-danish-royal-family)

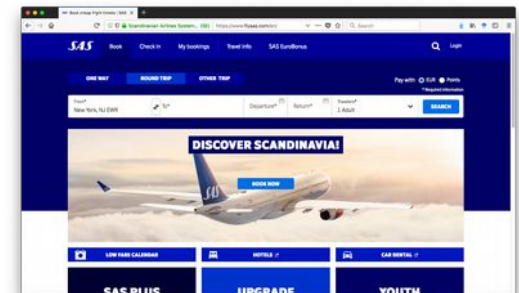
# Another exercise:

What *security goals* are relevant? Are there some goals that are the most important?

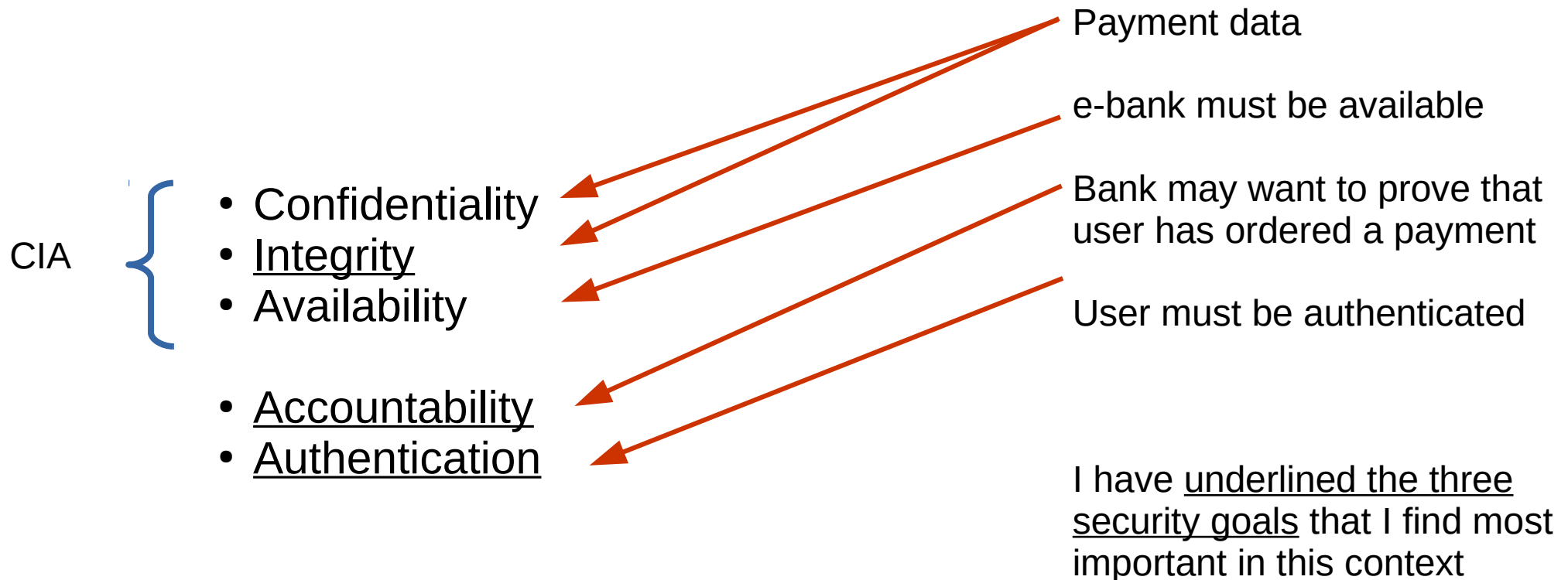
- CIA {
- Confidentiality
  - Integrity (data is authentic, not changed)
  - Availability
- 
- Authentication (verifying identity)
  - Accountability (not denying an action, non-repudiation)

The goals are mentioned in

- Pfleeger
- Rozansky and Woods (pp 442-446)
  - as “concerns”, though not including authentication



# Answer: what threat models and security goals are relevant?



# Literature

The Information Commissioner's Office. Encryption (p 3-4)

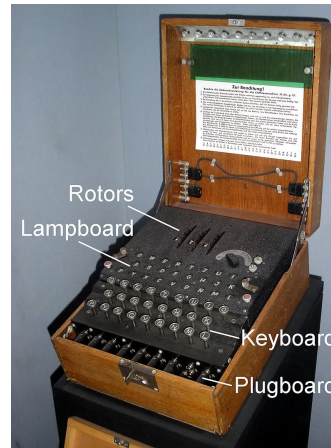
*“Encryption is a mathematical function using a secret value - the key - which encodes data so that only users with access to that key can read the information”*

*“Whilst it is possible to attempt decryption without the key [...], in practical terms it will take such a long time to find the right key (ie. many millions of years) that it becomes effectively impossible”*

Jon Callas. An Introduction to Cryptography (p 26)

*“In the end, NIST picked Rijndael to be the AES [...] an interesting result. Technically, Rijndael was the boldest design. [...] It showed that Kirchhoff’s principle [...] works.”*

# History of cryptography



Caesar  
cipher

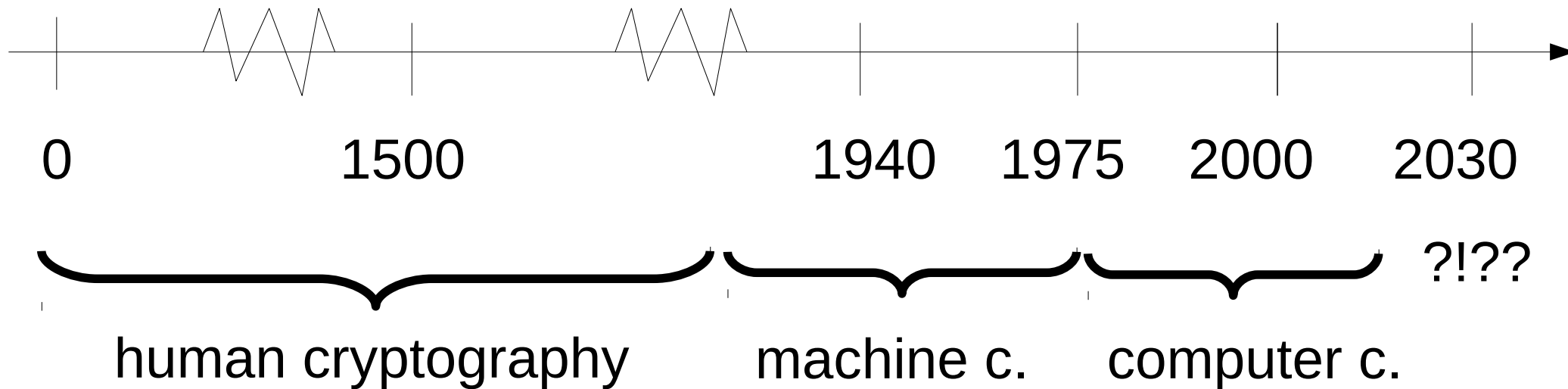
Vigenère  
cipher

Enigma

DES,  
RSA

AES

Quantum  
cryptogr.



# Security of encryption algorithms

Caesar (Antiquity)

- very insecure

Vigenère (~1500, see wikipedia)

- widely believed to be secure ~1500-1850
- however, some knew how to break it

Machine cryptography (ENIGMA and others)

- broken (but if improved they would have worked)

DES (1977)

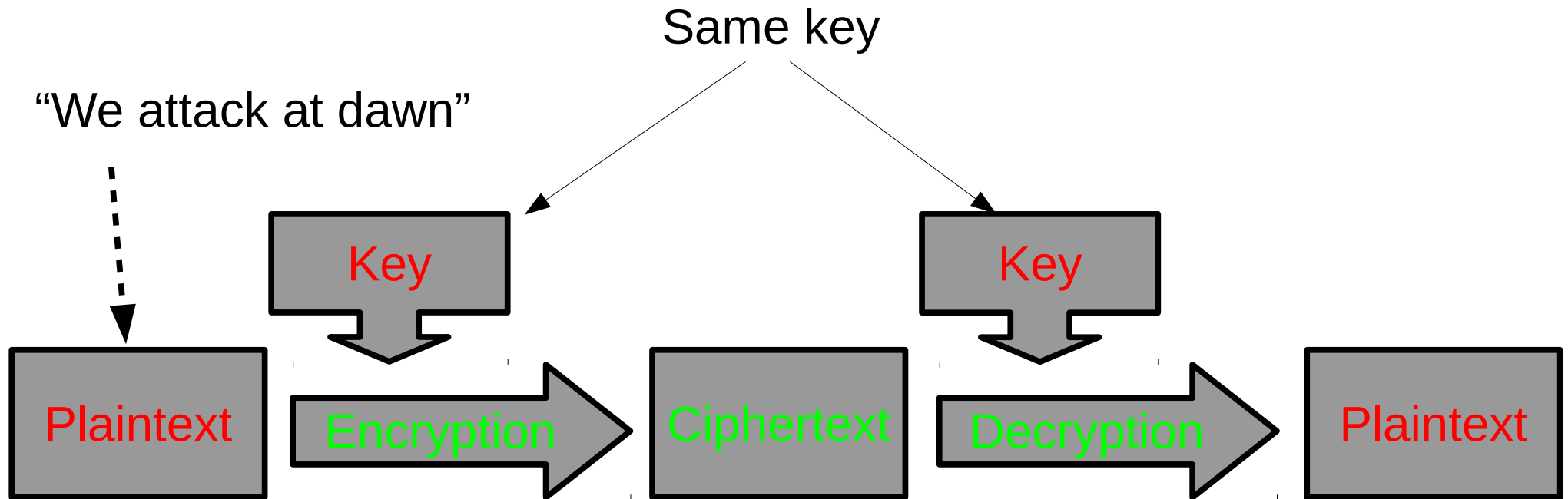
- suspicion about insecurity (NSA backdoor)
- in reality secure until about ~1990
- 3DES remains secure, but somewhat impractical

AES (2000)

- secure

# Symmetric encryption

- a single, secret key



Secret



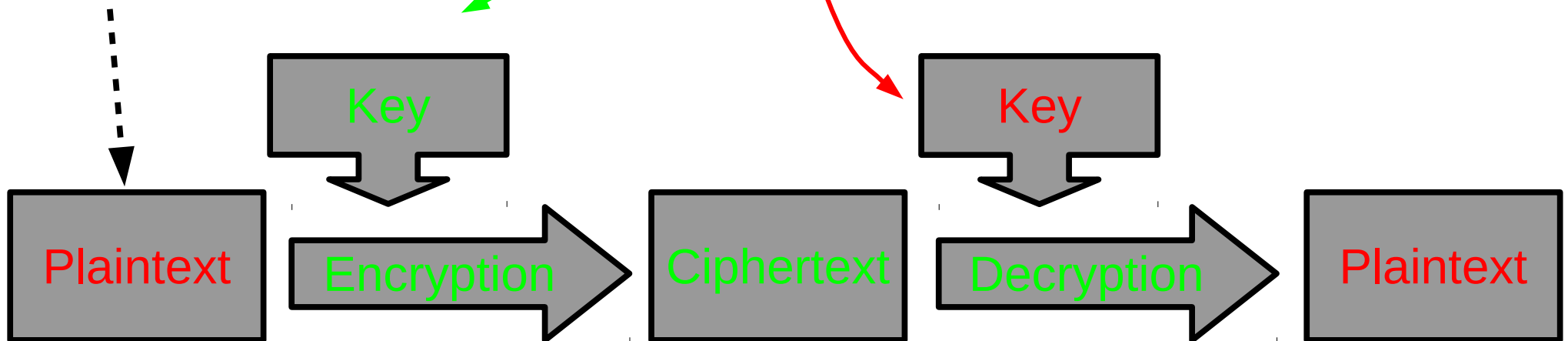
Public (encrypted)

# Asymmetric encryption

Two different keys

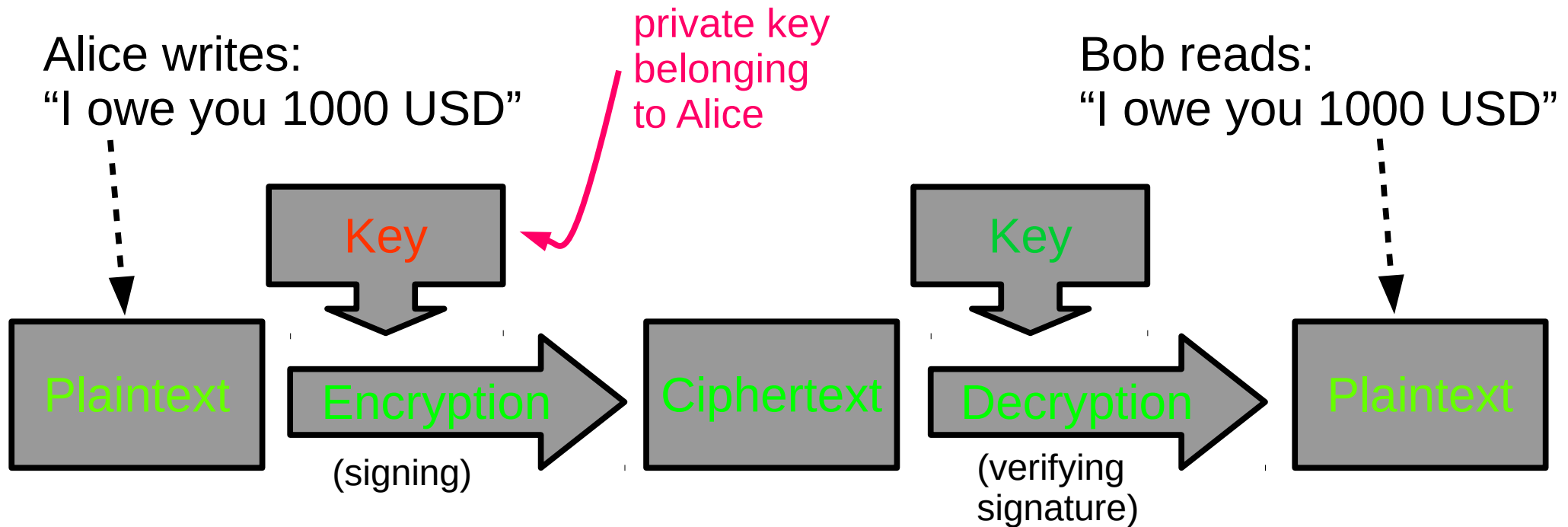
- 1 public
- 1 private (secret)
- private key only works with its corresponding public key

“We attack at dawn”





# Asymmetric encryption used reversely



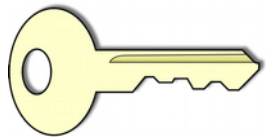
If Bob decrypts the ciphertext with Alice's public key, this proves that Alice sent the message, because Alice is the only person in possession of Alice's private key.

Bob does not possess Alice's private key, so Bob could not have encrypted the message himself.

*OBS: the ciphertext is encrypted, but anyone can read it if they know Alice's public key.*

# Agenda today

1. Introduction to security with a focus on encryption



2. Symmetric encryption

3. Asymmetric encryption



*“Basic cryptography”*

4. Exercise: PIA of your project => encryption?

5. Introduction to next time: *“Applied cryptography”*

# Human cryptography: Caesar cipher (a substitution algorithm)

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



IBM  
-> HAL

Algorithm:

- encryption: replace any character (for example B) with character in alphabet below (A in the example)
- decryption: the reverse process

Key:

- number of characters (for example 1) that lower alphabet has been moved to the right

# Exercise

Encrypt BUITA  
with key = 3.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

BUITA

-> ??????

# Answer

ABCDEFGHIJKLMN OPQRSTU VWXYZ  
XYZABCDEFGHIJKLMN OPQRSTU VW

BUITA

-> YRFQX

# Terminology

ABCDEF GHI JKLMNOPQRSTU VWXYZ  
XYZABCDEF GHI JKLMNOPQRSTU VW

Cryptology = cryptography + cryptanalysis

cryptography:

- protecting, defending data, designing algorithms
- all security goals: confidentiality etc.
- the art or science of ~
- technologies for ~

cryptanalysis:

- unveiling, attacking data, breaking algorithms
- art / science / technologies of ~
- is generally considered ethical: research, test, publish with delay

# Cryptanalysis

Here is an message encrypted using the Caesar method

- encrypted message: cipher text
- partial information about the plaintext: it is in English

CAMZAAPWCTLJMUILMIEIZM

*Cryptanalysis* is to find the original message

- original message = the so-called plaintext
- cryptanalysis = attack

# Attack method: brute force

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

CAMZAAPWCTLJMUILMIEIZM

A brute force-method examines all possible values of the encryption key.

Exercise: *How would you do a brute-force attack, to find the plaintext that has been encrypted into “CAMZAA..” ?*



# Solution to exercise

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

CAMZAAPWCTLJMUILMIEIZM

1. Try each of the 26 keys
2. For each key, decrypt, and check if the resulting plaintext is in English

This works because:

- we knew that the plaintext was in English
- it is extremely unlikely that we arrive at an English plaintext by chance

# Attack method: frequency analysis

????????????????????  
CAMZAAPWCTLJMUILMIEIZM

1. In the ciphertext, find the letter that occurs most frequently (M)
2. Select the key that encrypts E to this letter
3. If this does not work, experiment with other frequent letters

Frequency data for English ([wikipedia.org/wiki/Letter\\_frequency](https://wikipedia.org/wiki/Letter_frequency))

- E: 13%
- T: 9%
- A: 8%
- H, I, R, S: 6-7%

# Brute force attack



How many different combinations must be tried in a brute-force attack on this lock?

# Literature for today (cont.)

Jon Callas. *An Introduction to Cryptography*.  
(Chapter 3: pages 15-27)

What were the two main criticisms of the DES algorithm?  
(according to Callas)

# Answer: DES (1977)

1) The key was too short (56 bits)  
(true)

2) NSA had inserted a “backdoor”  
(wrong)

# The DES-cracker (1998)

Built by EFF (privacy advocates)

- broke DES in 3 days
- cost \$ 1/4 mill.
- 1856 CPUs

DES-cracker contest

- 10.000\$ prize
- by RSA Security Inc.
- ciphertext:
  - 79 45 81 c0 a0 6e 40 a2..
- plaintext:
  - “It's time for those 128-, 192-, and 256 bit keys”.



# Strong encryption

Strong = “unbreakable in practice”,

“unbreakable”: can be defined by defining “breakable”:

The attacker can find plaintext if attacker knows

- algorithm + ciphertext
- and normally some properties of the plaintext
  - recognizability: some natural language
  - knowledge about specific parts, ie. “<html> .. </html>”

“in practice”:

The attacker is assumed to have access to very powerful, yet realistic computing and storage resources, and is given reasonable time (perhaps 10 days or 5 years)

For trust in strength:

- algorithm definition & design rationale must be public
- must have been subjected to public scrutiny

# Exercise

What are the major differences between DES and AES (Rijndael)?  
(according to Callas)



# Answer

What are the major differences between DES and AES (Rijndael)?  
(according to Callas)

	DES	AES (Rijndael)
Key size	56 bit	128 bit or more
Design rationale	Partly secret	Fully public
Origin	USA (IBM, NSA)	Europe (independ. research)
Selection process	Closed	Open competition
Speed	Reasonably fast	Very fast

# Agenda today

1. Introduction to security with a focus on encryption

2. Symmetric encryption

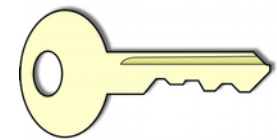
3. Asymmetric encryption



*“Basic cryptography”*

4. Exercise: PIA of your project => encryption?

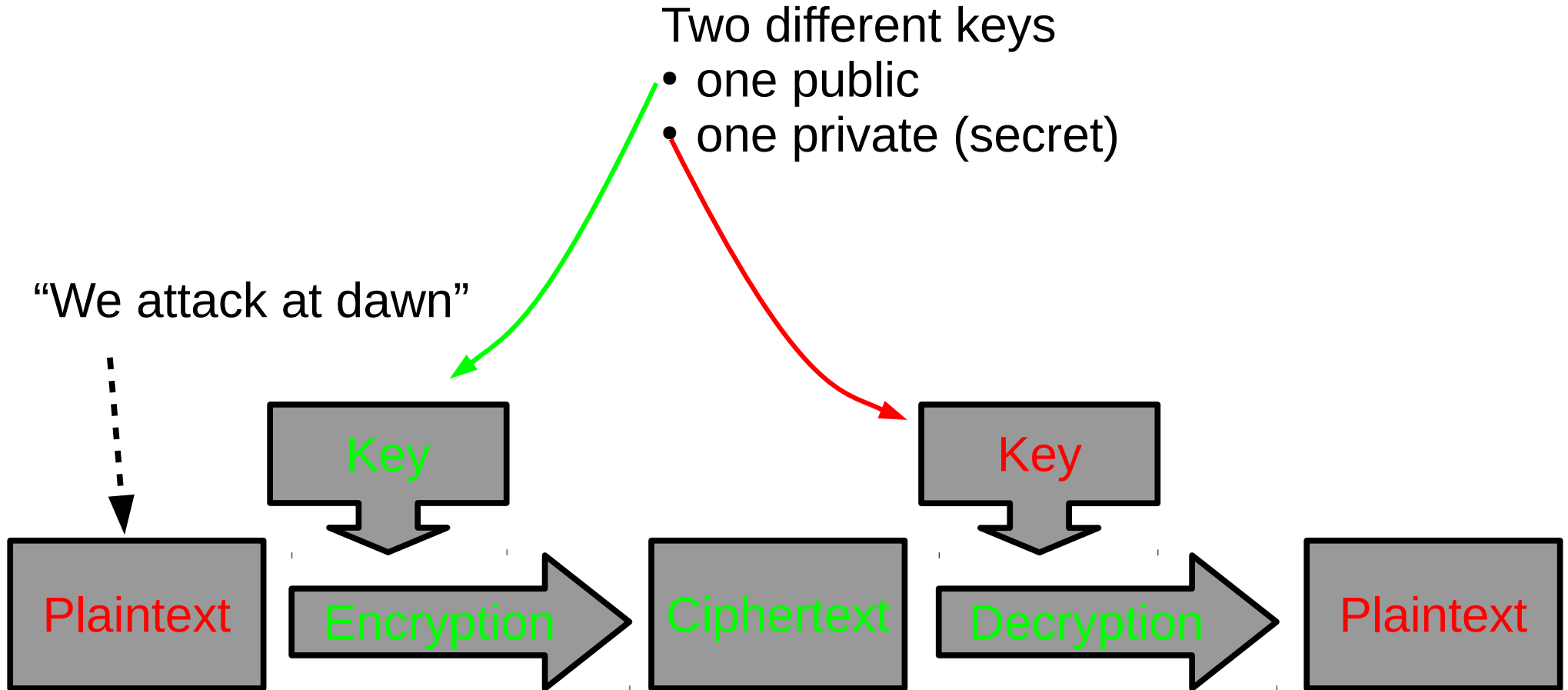
5. Introduction to next time: *“Applied cryptography”*



# Exercise:

What are the advantages and disadvantages of asymmetric encryption?  
(according Jon Callas)

# Asymmetric encryption



# Answer

What are the advantages and disadvantages of asymmetric encryption? (According to Callas)

Advantages: it solves the “key distribution problem”

- Bob’s public key can be sent from Bob to Alice
- so they don’t have to meet in person to exchange a key
  - or use a diplomat travelling with a suitcase (with the key)
- Proof of identity
  - if used reversely, the private key can be used for signing

Disadvantages:

- asymmetric encryption is complex
  - perhaps not a very serious disadvantage
- asymmetric encryption/decryption is slow
  - so merely used to transmit a key for symmetric encryption

# Asymmetric encryption is complex

Asymmetric encryption uses that some mathematical operations are easy to do in one direction, and complex in the opposite direction

Examples of operations that are easy/complex depending on “direction”

- multiplication is easy, division is complex  
 $11 * 13 = 143$  is easy  
 $143 / 13 = 11$  is complex
- taking numbers to a power is easy, finding a root is complex  
 $13^3 = 13 * 13 * 13 = 2197$  is easy  
 $\sqrt[3]{2197} = 13$  is complex

# Conclusion so far, with a view to your project

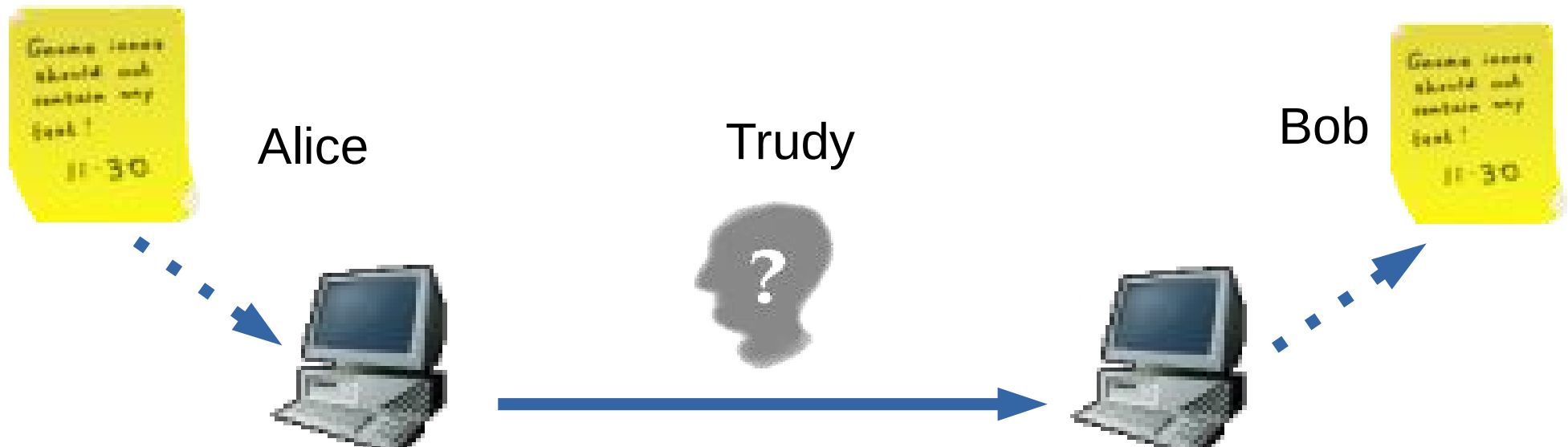
In your project, if you must send sensitive data from Alice to Bob:

Is it technically possible to protect confidentiality of data in transit or storage? *Yes!*

Can large amounts of data be encrypted fast? *Yes, with symmetric e.!*

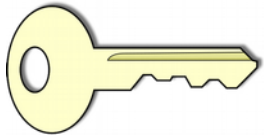
Is it possible to exchange a key for symmetric encr.?

- *Yes, if you send the new key using asymmetric encryption!*



# Agenda today

1. Introduction to security with a focus on encryption
  2. Symmetric encryption
  3. Asymmetric encryption
- } *“Basic cryptography”*
4. Exercise: PIA of your project => encryption?
  5. Introduction to next time: *“Applied cryptography”*





# Exercise

- (A) Identify one to three privacy risks in your project
- (B) Select a risk, and suggest a solution to eliminate or reduce it
- (C) Present to class (one risk, one solution)

# Suggested formats (focus on red items)

(A) Identify three privacy risks in your project

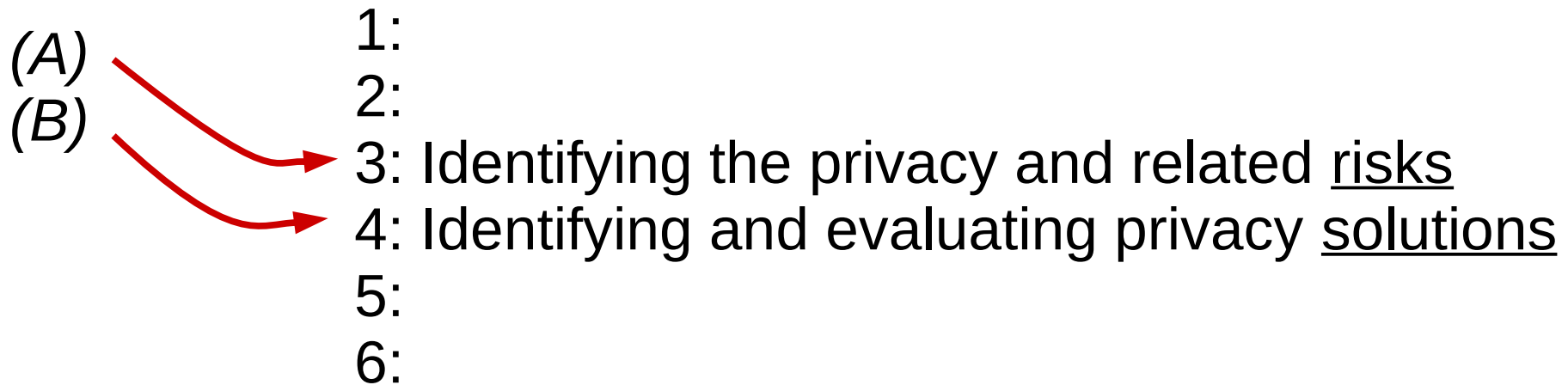
#	Privacy issue	Risk to individuals	Compliance risk	Organization risk
1	Disclosure of data about purchases made by users (including celebrities)	The individuals whose purchases may be disclosed	EU's GDPR	Damage to Nets and IBM
2	....			
3	....			

(B) Suggest solutions to eliminate or reduce a selected risk

Risk	Solution	Result	Evaluation
#1 ..	.. encryption? access control? ....	Eliminated? reduced?	Too complex? (endangers usability)

Format is from ICO's paper "Conducting privacy impact assessment. Code of practice", p36-37

# Exercise (A) and (B) corresponds to stages 3 and 4 in PIA process (as defined in ICO paper, p15)



# Recall from ICO-paper “*Conducting privacy impact assessments code of practice*” (lecture 3)

A / Stage 3 (p 33)

Questions 1-8, including (e.g.) “*Will information [...] be disclosed to [...] people who have not previously had routine access [...]?*”

B / Stage 4 (p27-28)

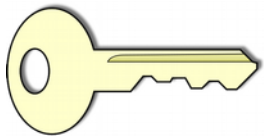
*“[...] the aim of a PIA is not to completely eliminate the impact on privacy. The purpose of the PIA is to reduce the impact to an acceptable level”*

“Measures include:

- Deciding not to collect or store ..
- Implementing technological security measures
- Staff training
- Anonymise the information
- ..”

# Agenda today

1. Introduction to security with a focus on encryption
  2. Symmetric encryption
  3. Asymmetric encryption
- } *“Basic cryptography”*
4. Exercise: PIA of your project => encryption?
  5. Introduction to next time: *“Applied cryptography”*



# Course literature for Thursday, October 11<sup>th</sup>

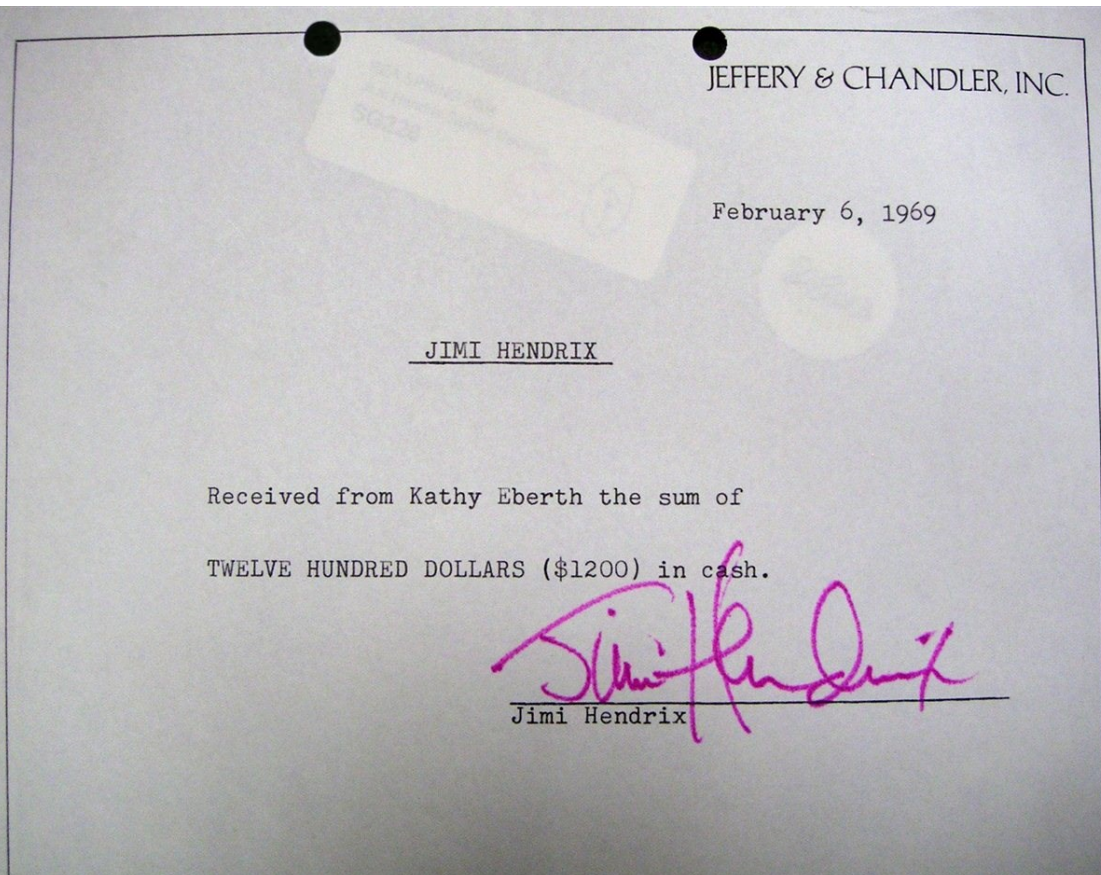
The European Commission: *EU's General Data Protection Regulation (GDPR)*. The document is about 250 pages. Please read Article 6 (Lawfulness of processing) and Article 32 (Security of processing), which is a total of about five pages.

Wikipedia: *Cryptographic hash function*. Please read the introduction and the section "Properties" and try to understand the three properties "Pre-image resistance", "Second pre-image resistance" and "Collision resistance". Also study the image on top of the Wikipedia page. (The page was accessed October 3rd, 2018).

David Youd. *What is a digital signature?* About four pages.

A. Whitten & J.D Tygar. *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. 1999. (16 pages). The most important sections are 1-4 (about 9 pages).

# Digital signatures resemble paper-based signatures



Properties of digital and physical signatures

- originality of document is protected
- authenticity of signer is protected
- links document and signer

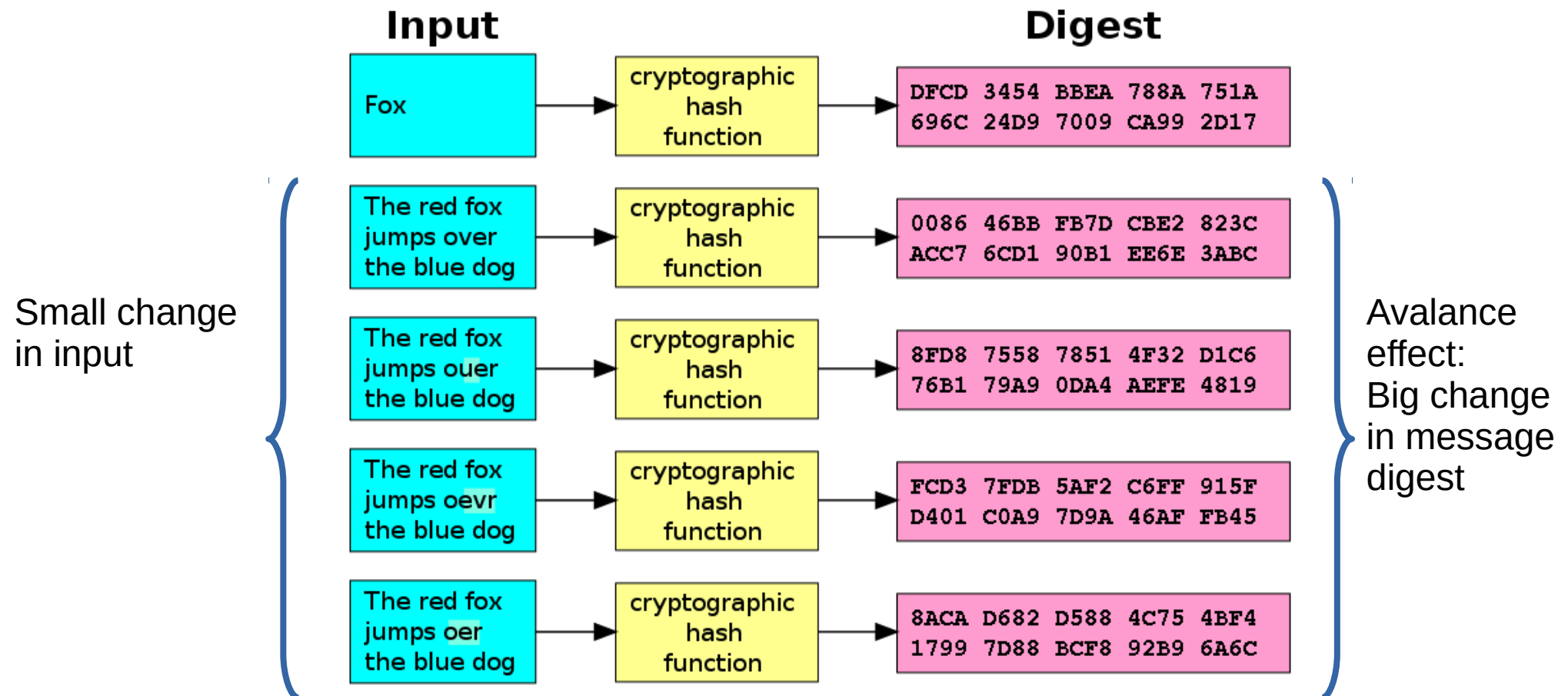
Digital signatures

- created using signer's private key
- confirmed using signer's public key

# Wikipedia: Cryptographic hash functions

A message digest is the output of a cryptographic hash function

Message digests have “avalanche property”





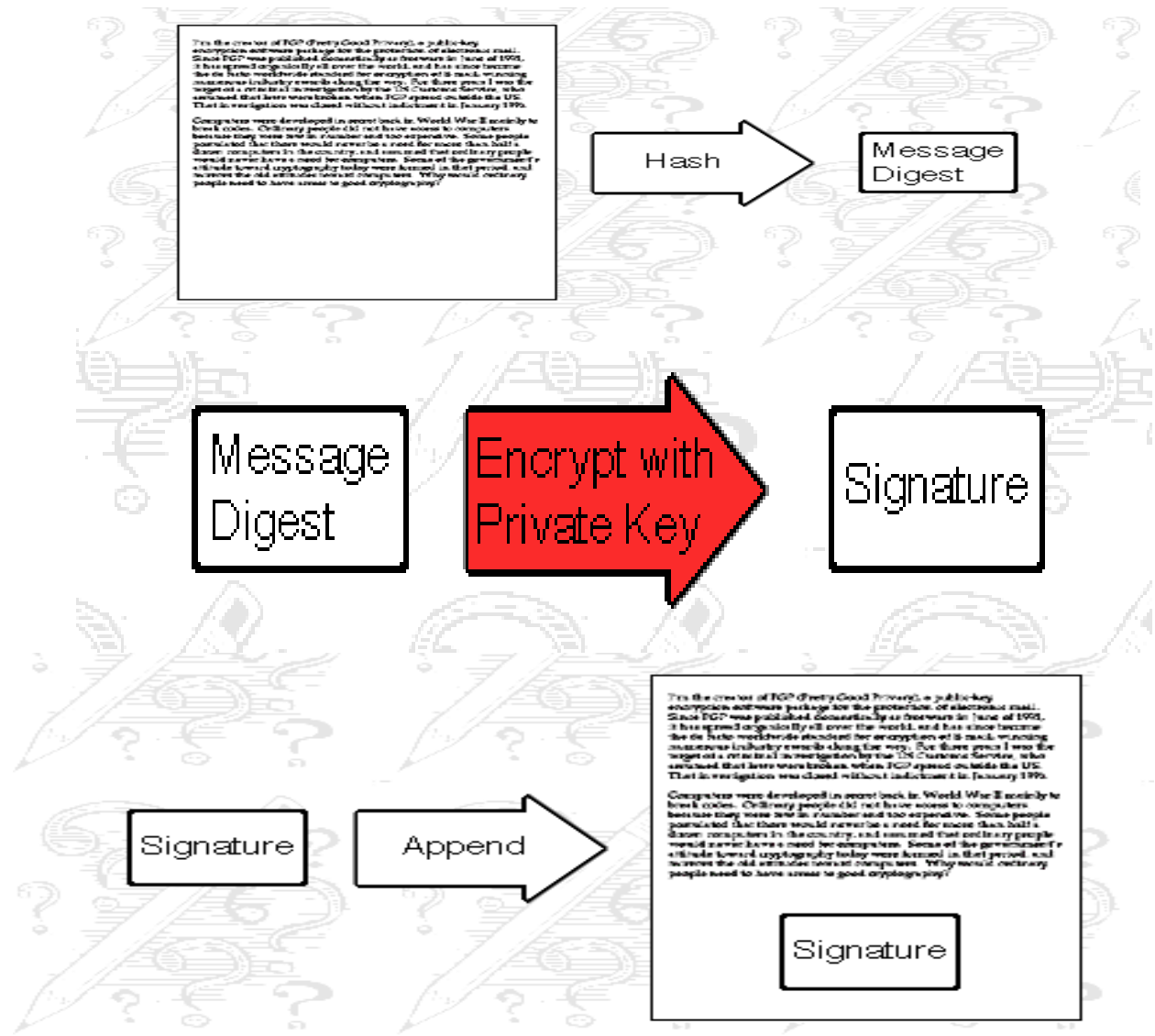
# Digital signature produced by sender

Bob (signer, sender)

1. Compute message digest

2. Compute signature with private key

3. Append signature to document, then send.



# Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten

*School of Computer Science*

*Carnegie Mellon University*

*Pittsburgh, PA 15213*

*alma@cs.cmu.edu*

J. D. Tygar<sup>1</sup>

*EECS and SIMS*

*University of California*

*Berkeley, CA 94720*

*tygar@cs.berkeley.edu*

## Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

To test this hypothesis, we performed a case study

## 1 Introduction

Security mechanisms are often not used correctly. Strong cryptographic protocols, and bug-free code notwithstanding, the people who use the software do not click the encrypt button when they need to use a communication protocol because they are confused about which cryptographic key to use, or they accidentally configure their software incorrectly. To make their private data work, they use mechanisms such as these are already qu