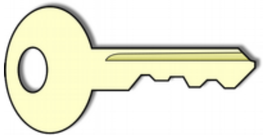
Basic cryptography

BUITA lecture 8
March 15th, 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 today

Specific learning goals (moodle)

- 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

Learn from exercise: PIA of your project => encryption?

- identify values, threats, and countermeasures in IT projects
- security risk assessment on a specific it system architecture

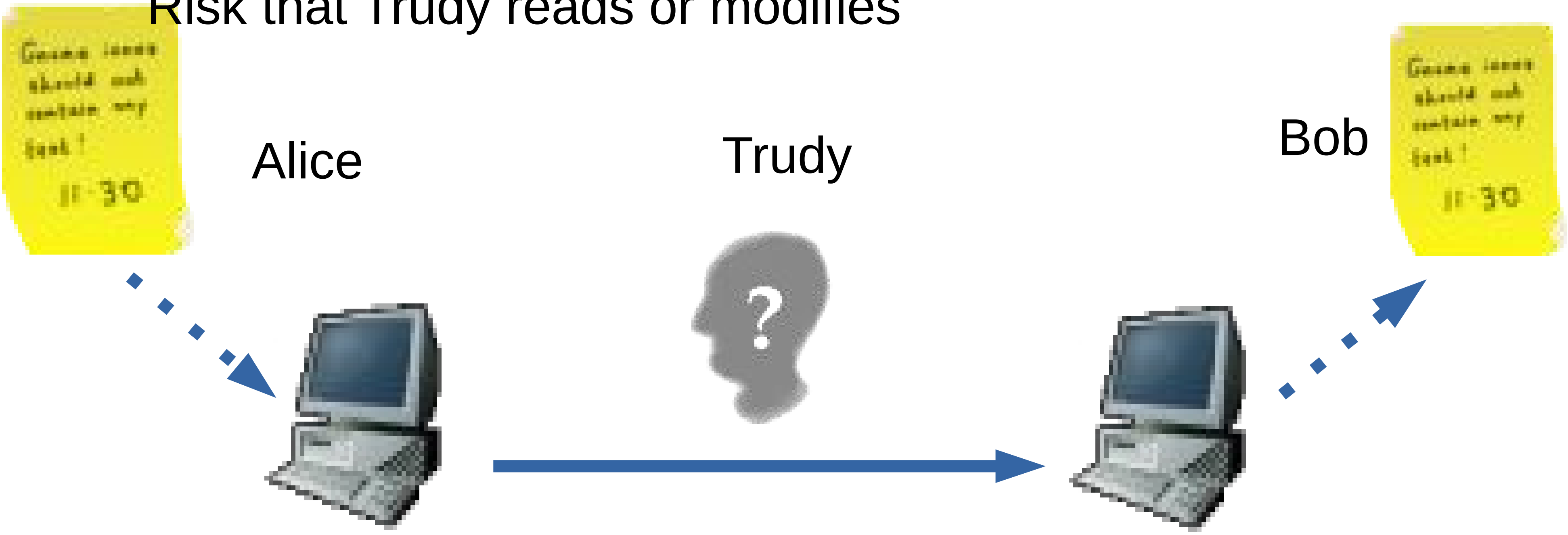
Threat model 1: Transmitted data

Data sent from Alice to Bob

- Bob and Alice are persons
- or sometimes a program

We assume that data is sent over unprotected network

Risk that Trudy reads or modifies

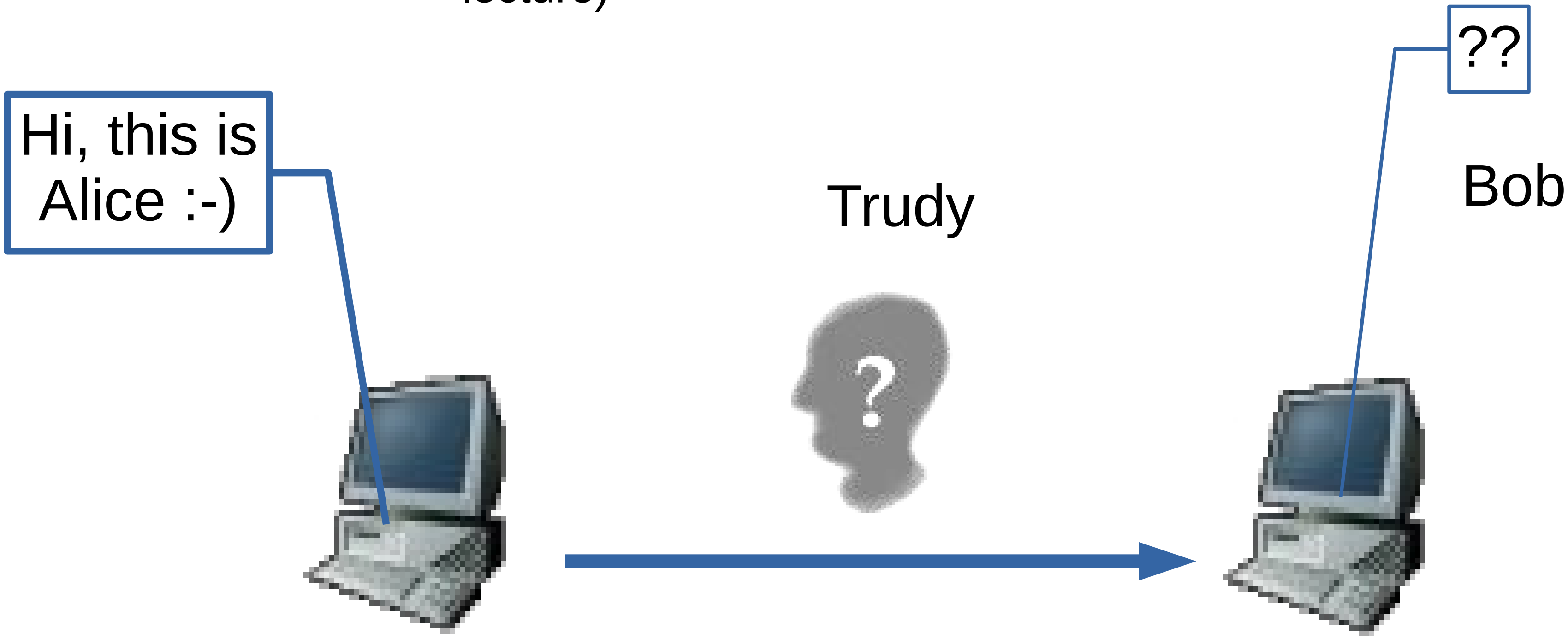


Threat model 2:
Stored data

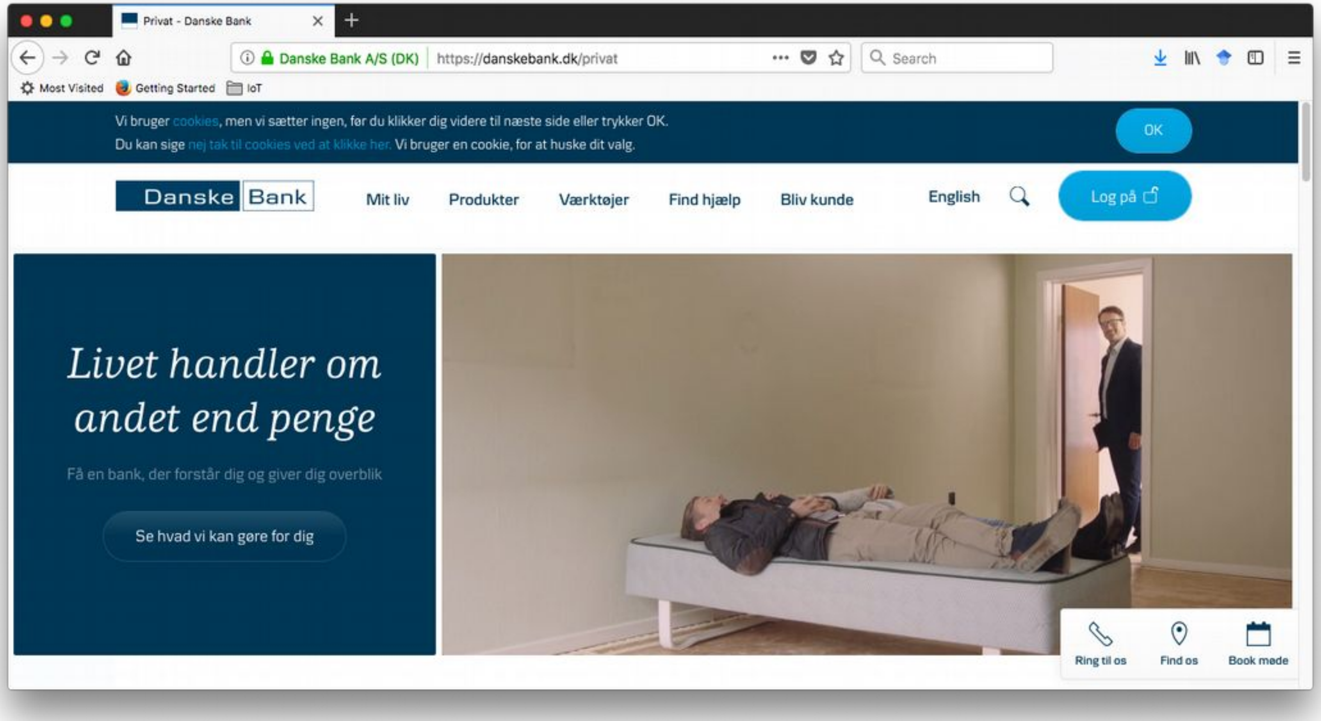
Alice has legitimate access to Bob (Bob’s stored data)

There is a risk that someone (Trudy) pretends to be Alice, and thereby gains access to Bob’s stored data

(Threat model 2 will be covered in more detail in the next lecture)



e-banking



Vi bruger cookies, men vi sætter ingen, før du klikker dig videre til næste side eller trykker OK.
Du kan sige nej tak til cookies ved at klikke her. Vi bruger en cookie, for at huske dit valg.

Livet handler om andet end penge

Få en bank, der forstår dig og giver dig overblik

You log-on to your e-bank, to order a transfer of money, say, to the seller of an item you have bought on ebay

Exercise:

- *Is threat model 1 relevant?*
- *Is threat model 2 relevant?*

Answer:
what threat models are relevant?

Threat model 1 (transmitted data): Relevant

- your transfer order is transmitted over the Internet or themobile network

Threat model 2 (stored data): Relevant

- someone could get access to your account at the netbank
- in addition to protecting your account data from being read,
  this is also about protecting against someone stealing money from you

Another exercise:

What *security goals* are relevant?

CIA

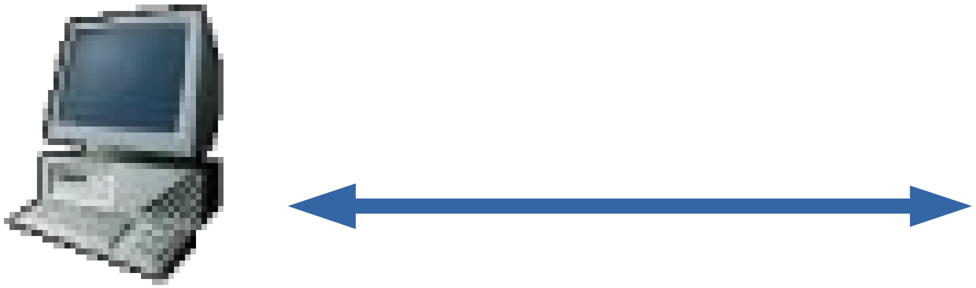
- Confidentiality
- Integrity (data is authentic, not changed)
- Availability

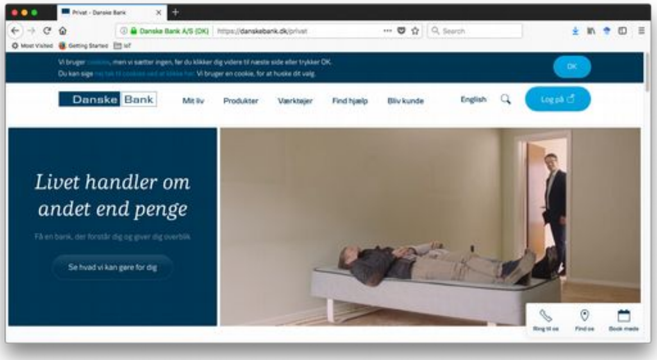
- Accountability (not denying an action, non-repudiation)

Also important, though not mentioned in the overview of concerns in Rozansky and Woods (pp 442-446):

- Authentication (verifying indentity)

Alice



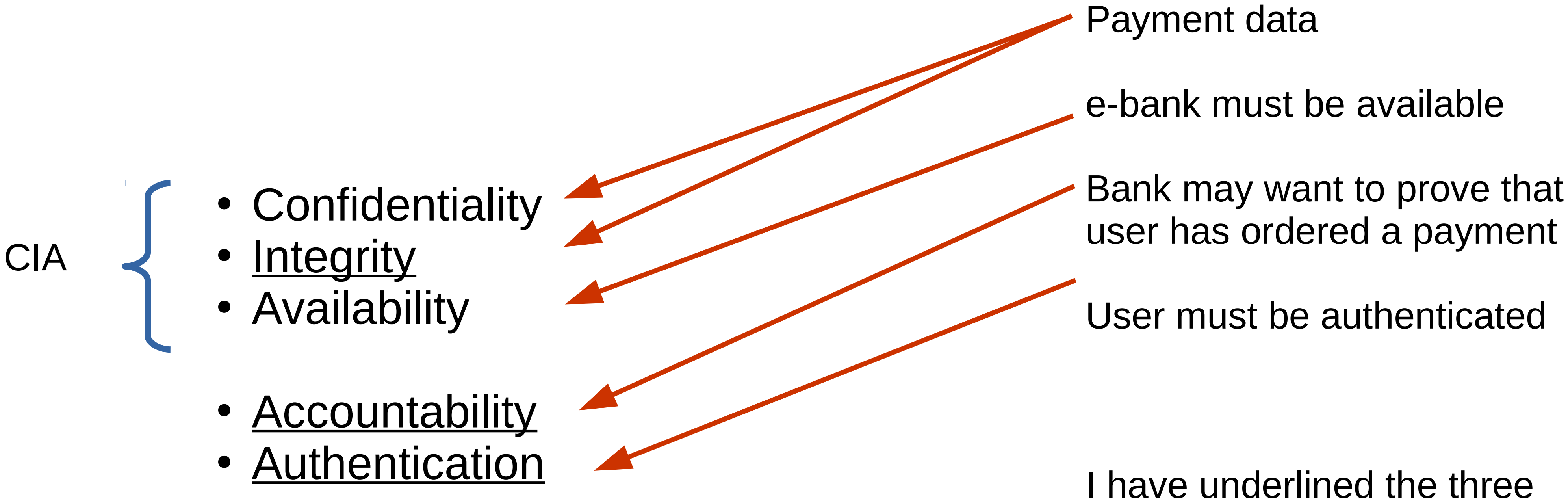


Vi bruger cookies, men vi sætter ingen, før du klikker dig videre til næste side eller trykker OK.
Du kan sige nej tak til cookies ved at klikke her. Vi bruger en cookie, for at huske dit valg.

Livet handler om andet end penge

Få en bank, der forstår dig og giver dig overblik

Answer: what threat models and security goals are relevant?



CIA

- Confidentiality
- Integrity
- Availability

- Accountability
- Authentication

Payment data

e-bank must be available

Bank may want to prove that user has ordered a payment

User must be authenticated

I have underlined the three security goals that I find most important in this context

Literature for today

The Information Commissioner's Office (ICO) in the UK.
Encryption.
(Please read pages 1-14.)

> *“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” (p3)*
>
> *“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” (p4)*

Residual risks with

1. Encrypted data storage?
2. Encrypted data transfer?

Answers about residuals risks

1. Encrypted data storage?

- If a user leaves the computer while logged on..

(ie. while the data is unencrypted)

- Encryption does not protect against destruction of data

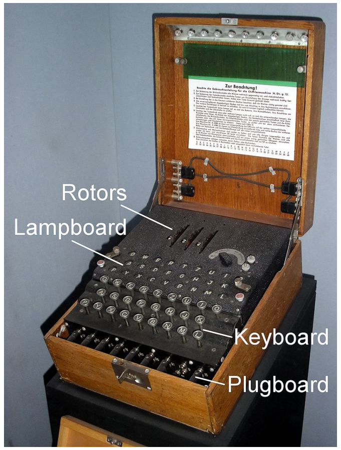
- If applications have access to data (ie. a webservice having access to decrypt), an attack may try to attain the privileges of the webservice

2. Encrypted data transfer?

- Metadata is not encrypted (sender, receiver, size, time, ..)

- How to trust endpoints? (certificates)

Encryption protects transmitted data



Caeser cipher

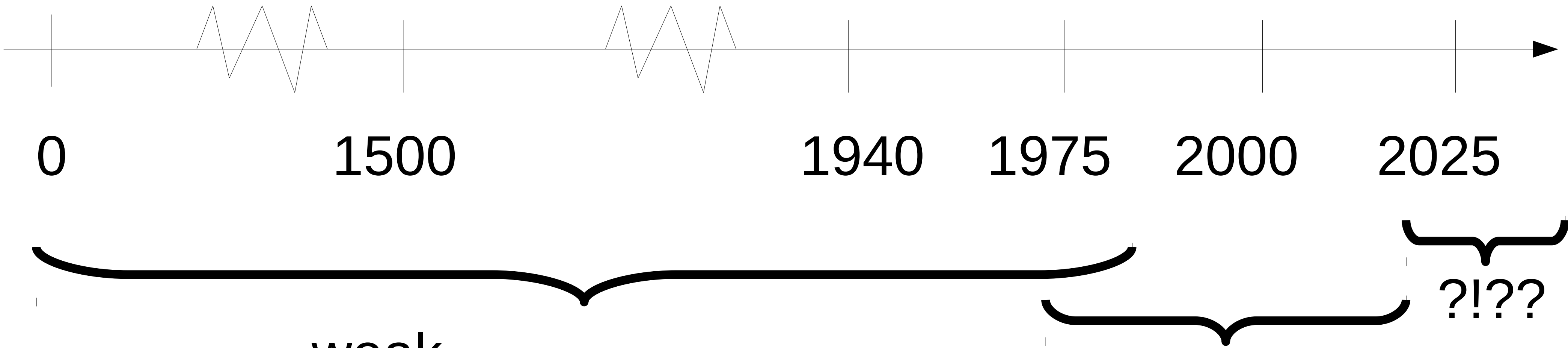
Vigenère cipher

Enigma

DES, RSA

AES

Quantum cryptogr.



0

1500

1940

1975

2000

2025

weak

strong

?!??

Security of encryption algorithms

Caesar (Antiquety)
- very insecure

Vigenère (~1500, see wikipedia)
- widely believed to be secure ~1500-1850
- however, some knew how to break it

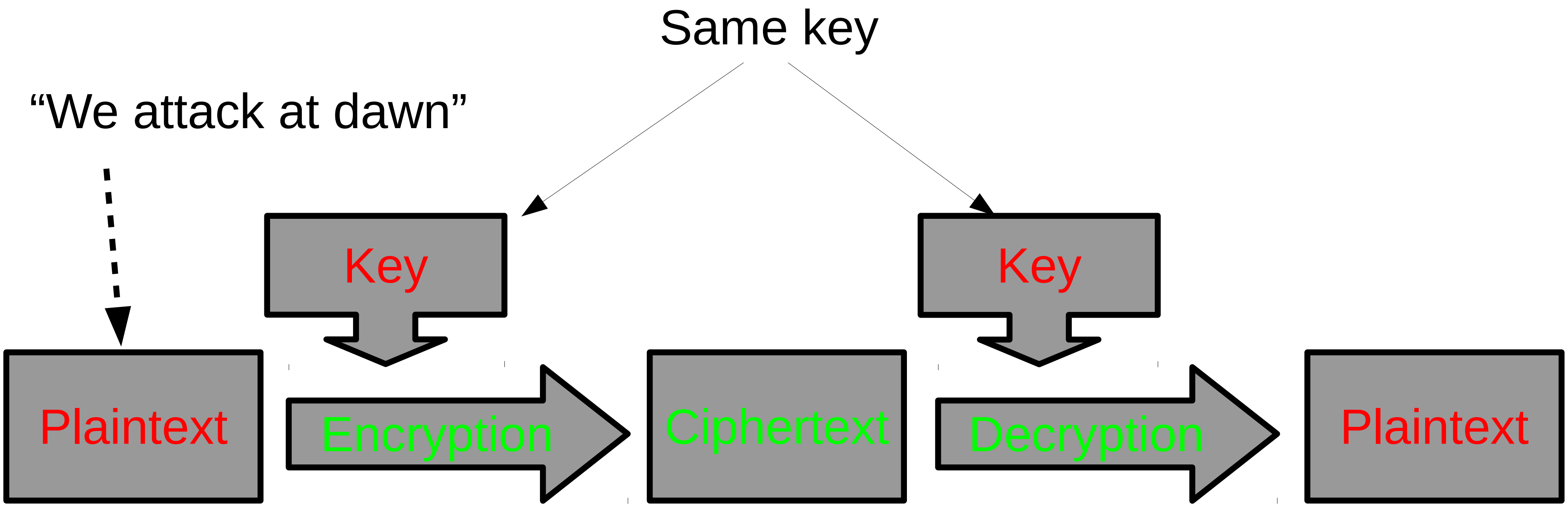
Machine cryptography (ENIGMA and others)
- broken (but if improved they would have worked)

DES (1977)
- suspicion about insecurity (NSA backdoor)
- in reality secure until about ~1990
- 3DES remains secure, but somewhat impractical

AES (2000)
- secure

Symmetric encryption

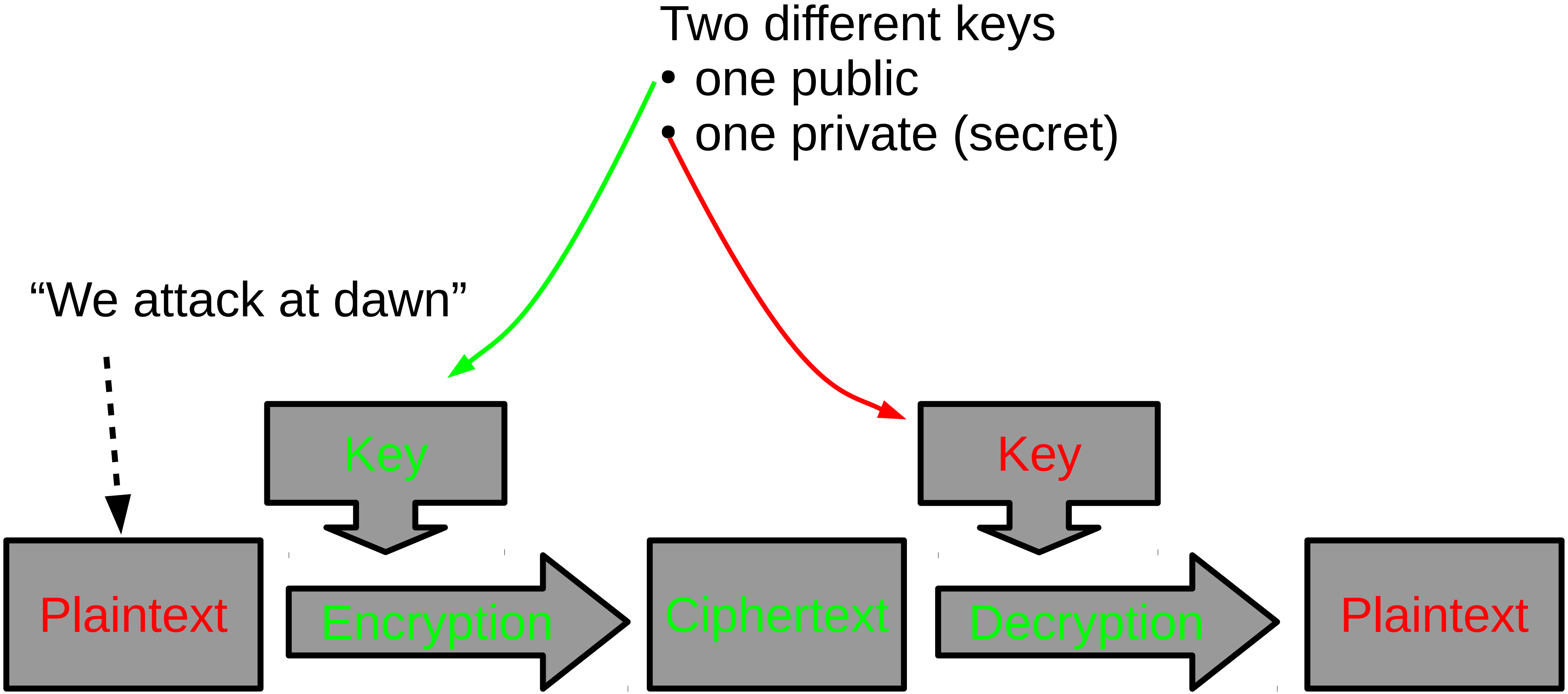
- a single, secret key



🟥 Secret

🟩 Public (encrypted)

Asymmetric encryption



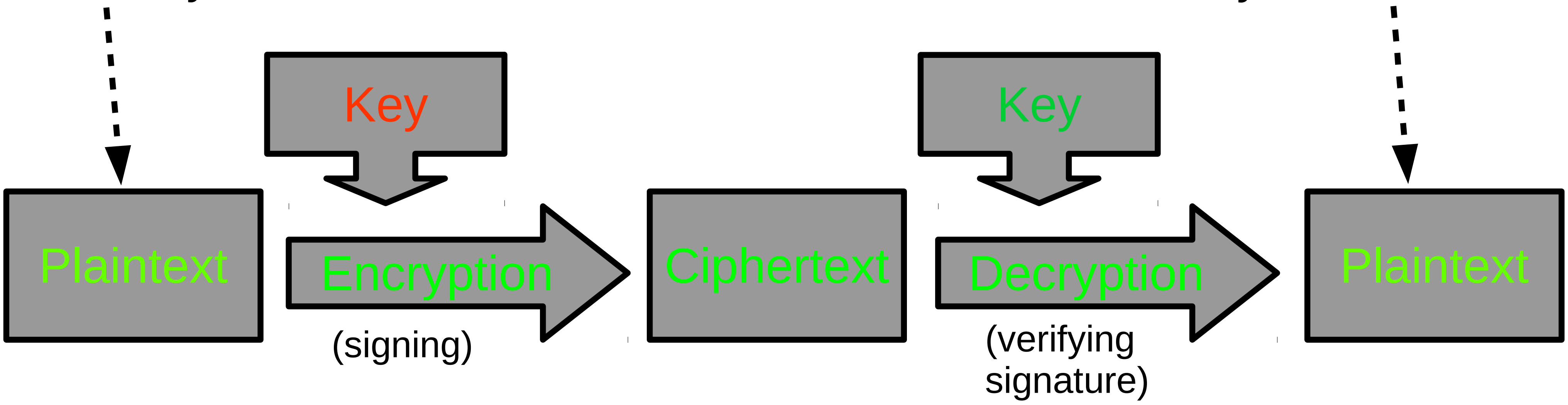
Two different keys
- one public
- one private (secret)

“We attack at dawn”

Asymmetric encryption used reversely

Alice writes:
“I owe you 1000 USD”

Bob reads:
“I owe you 1000 USD”



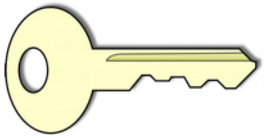
If Bob decrypts the ciphertext with Alice’s public key,
this proves that Alice sent the message,
because Alice is the only person in possession of Alice’s private key.

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 publc 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 example: Caesar cipher (a substitution algorithm)

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZABCDEFGHIJKLMNOPQRSTUVWXY

IBM
-> HAL

Algorithm:

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

Key:

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

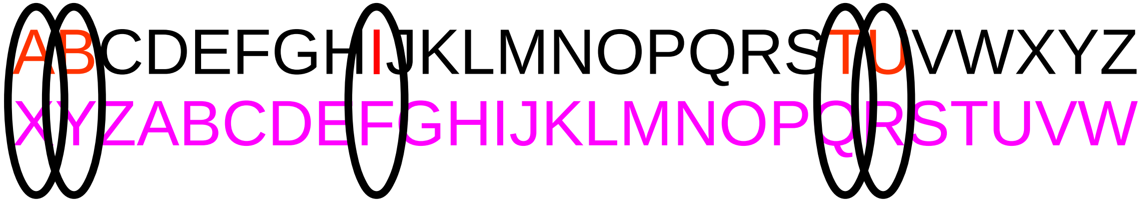
Exercise

Encrypt BUITA
with key = 3.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

BUITA
-> ?????

Answer



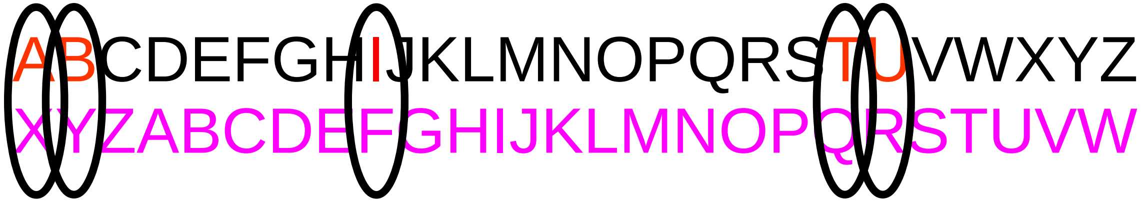
ABCDEFGHIJKLMNOPQRSTUVWXYZ

XYZABCDEFGHIJKLMNOPQRSTUVW

BUITA

-> YRFQX

Terminology



ABCDEFGHIJKLMNOPQRSTUVWXYZ

XYZABCDEFGHIJKLMNOPQRSTUVW

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
- and in this case: a *known* 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

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

This works because the proportion of letter sequences that are English words/sentences is extremely low

Attack method: frequency analysis

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

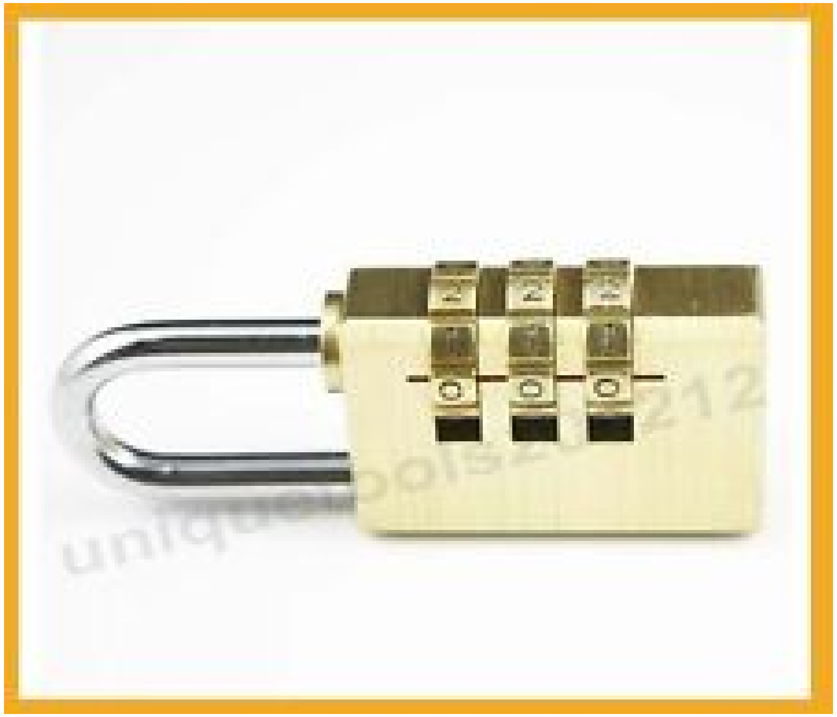
CAMZAAPWCTLJMUILMIEIZM

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)

- 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 powerfull, yet realistic computing and storage ressources, 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

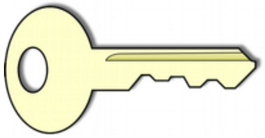
What are the major differences between DES and AES (Rijndael)? (according to Callas)

	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?

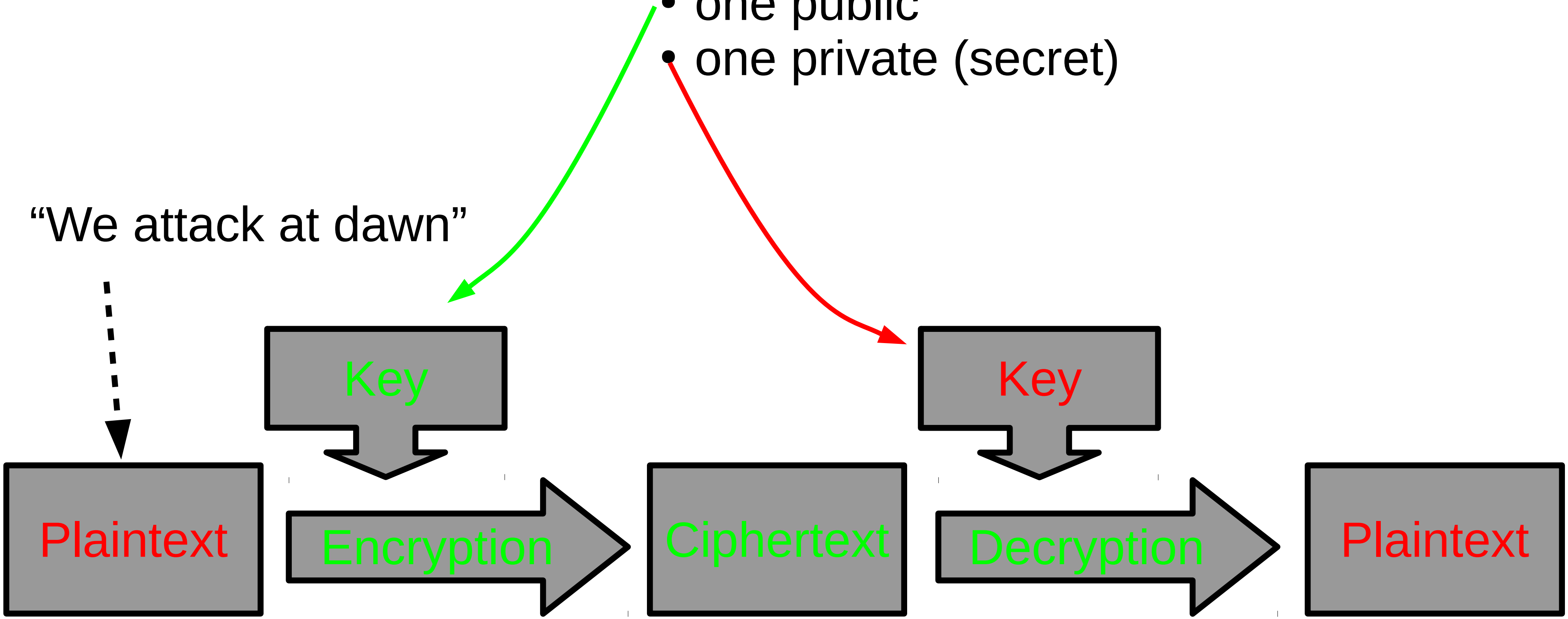
5. Introduction to next time: *“Applied cryptography”*

Exercise:

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

Asymmetric encryption

Two different keys
- one public
- one private (secret)



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 kan be used for signing

Disadvantages:

- asymmetric encryption is complex
  - perhaps not a very serious disadvantage
- (also, asymmetric encryption/decryption is very slow
  - so often used to transmit a key for symmetric encryption)

Asymmetric encryption is complex

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

For example:

- multipication 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; $\sqrt[3]{2197}$ = 13 is complex

RSA, a kind of asymmetric encryption, uses a product of prime numbers as part of the public key

- for example, the product 11*13 = 143

An attacker can break the encryption if he can find the factors 11 and 13 of 143 (of course real examples have larger numbers)

Conclusion so far, with a view to your project

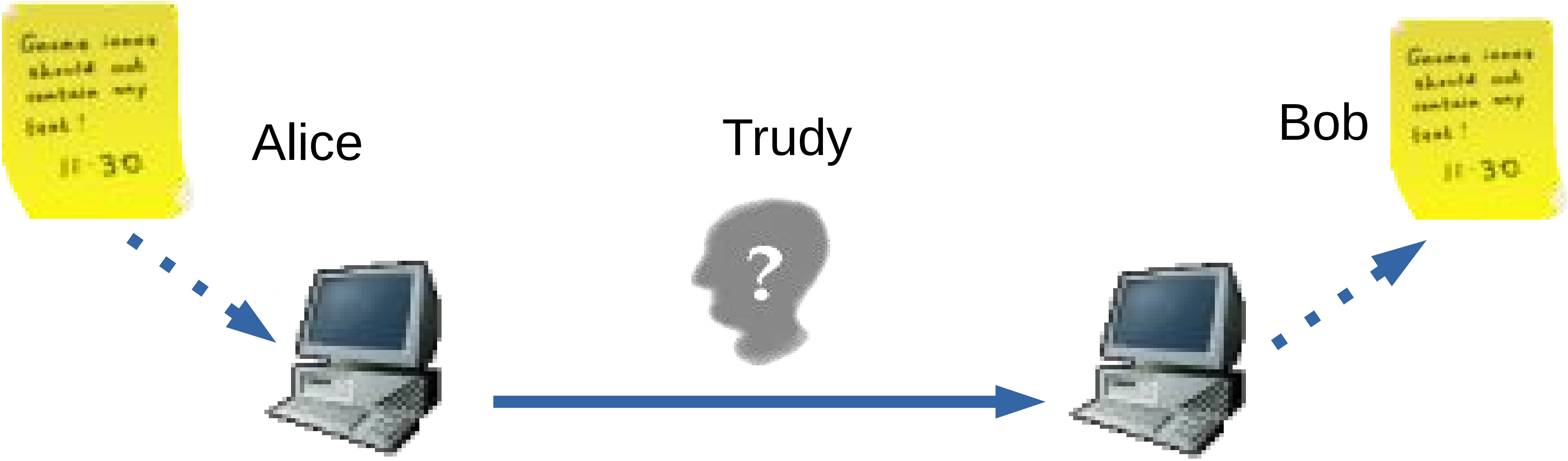
In your project, if you must send sensitive data from Alice to Bob:

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

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

Is it possible to change a key for symmetric encr., say once every day?

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



Alice

Trudy

Bob

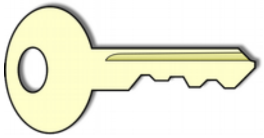
Agenda today

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 absense data - stored - transient	Employees whose absence data is stored / transmitted	EU Data Directive DK Persondataloven	Damage to image? Fines?
2	....			
3	....			

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

Risk	Solution	Result	Evaluation
#2 ..	.. 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)

(A)
(B)

1:
2:
3: Identifying the privacy and related risks
4: Identifying and evaluating privacy solutions
5:
6:

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

A / Stage 3 (p 33)

Questions 1-8

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

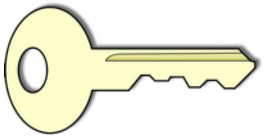
1. Introduction to security with a focus on encryption

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 Tuesday, March 22nd

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.

David Youd. *What is a digital signature?* About four 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 "Collission resistance". Also study the image on top of the Wikipedia page. (The page was accessed March 14, 2018).

Threat model 2

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).

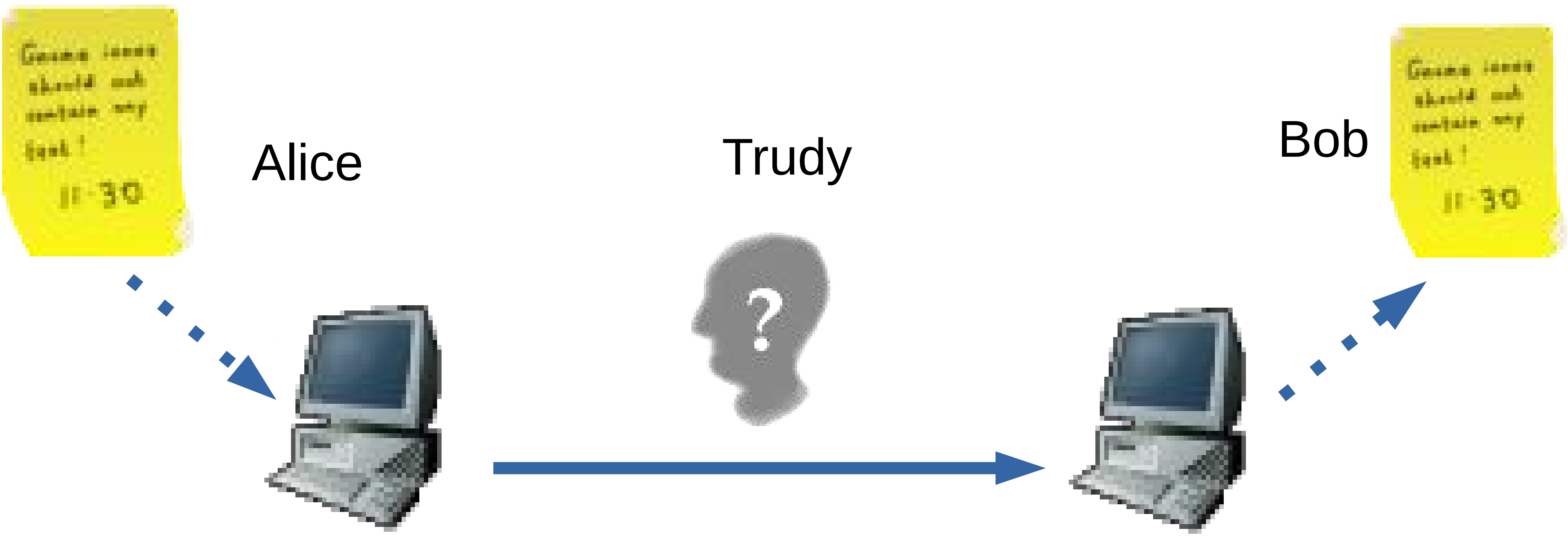
Threat model 1: Transmitted data

Data sent from Alice to Bob

We assume that data is sent over unprotected network

Risk that Trudy reads or modifies

Encryption is useful for protection of transmitted data.



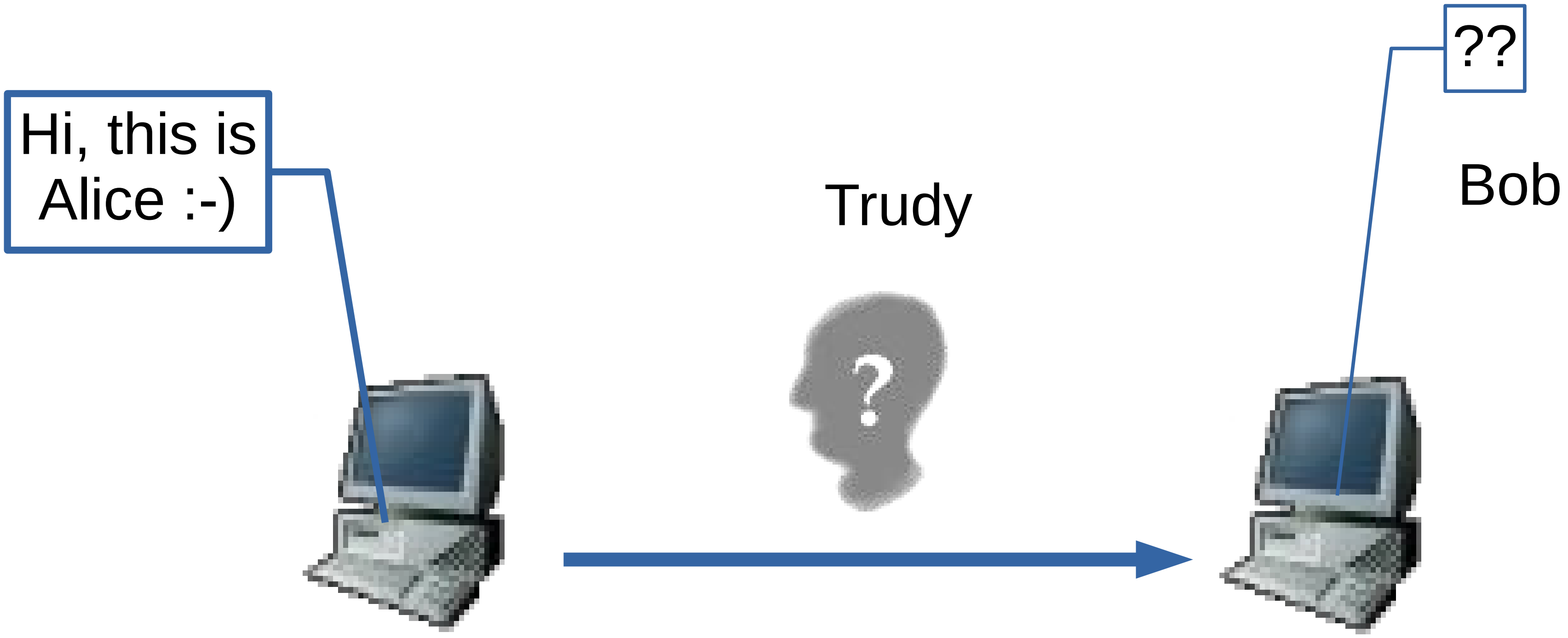
Alice

Trudy

Bob

Monday, October 23rd
Threat model 2: Stored data

Encryption is useful also for protection of stored data; but in addition, we have to consider how to prevent Trudy from pretending to be Bob, and thereby getting access to
(1) Not only Bob’s unencrypted data
(2) But possibly also Bob’s encrypted data



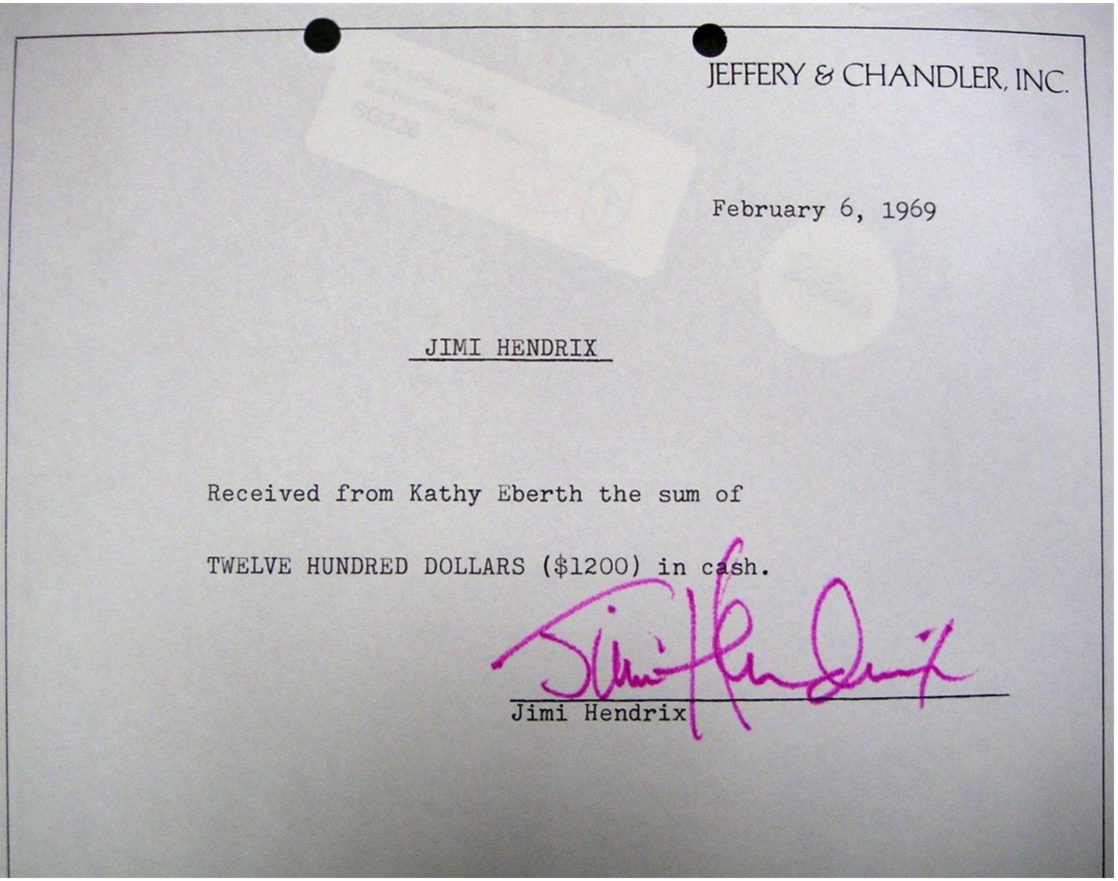
Hi, this is Alice :-)

Trudy

??

Bob

Digital signatures resemble paper-based signatures



JEFFERY & CHANDLER, INC.

February 6, 1969

JIMI HENDRIX

Received from Kathy Eberth the sum of

TWELVE HUNDRED DOLLARS ($1200) in cash.

Jimi Hendrix

Jimi Hendrix

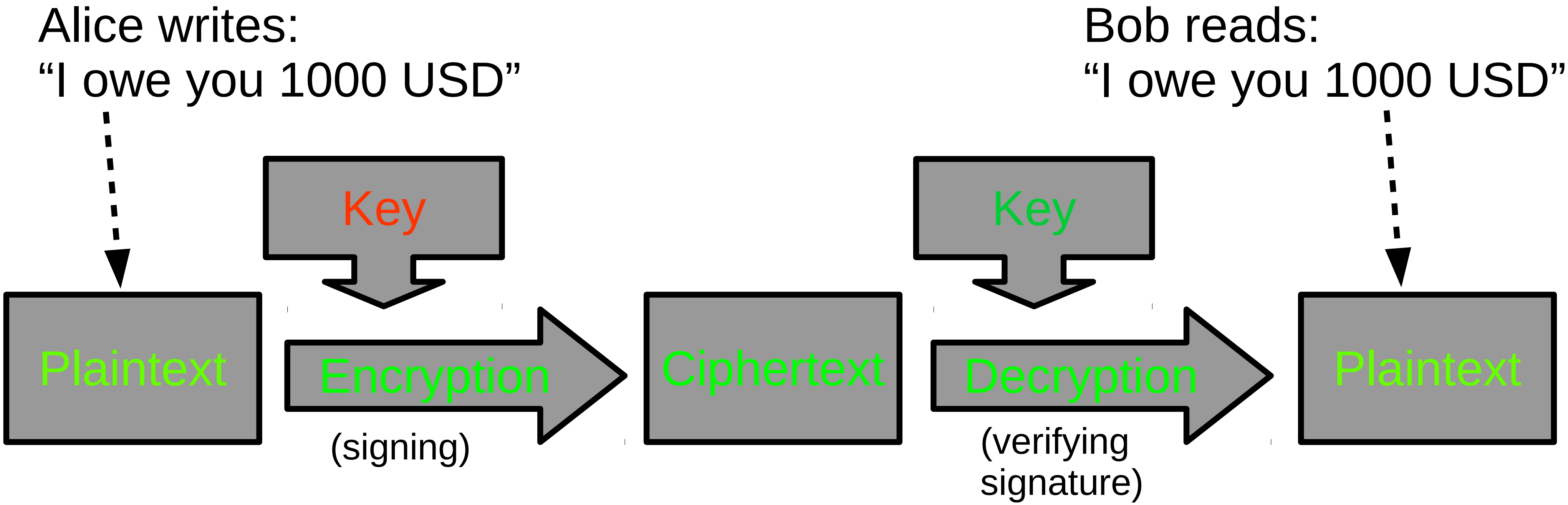
Properties of digital and physical signatures

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

Digital signatures

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

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 publc key.

Cryptograhpic hashing

Cryptographic hashing is used in digital signatures
(not shown on the previous slide).

So:

- encryption with the signer’s private key is applied to a *hash value of the document* (not the document itself)
- a digital signature (of a document) is a signed hash value (of the document)

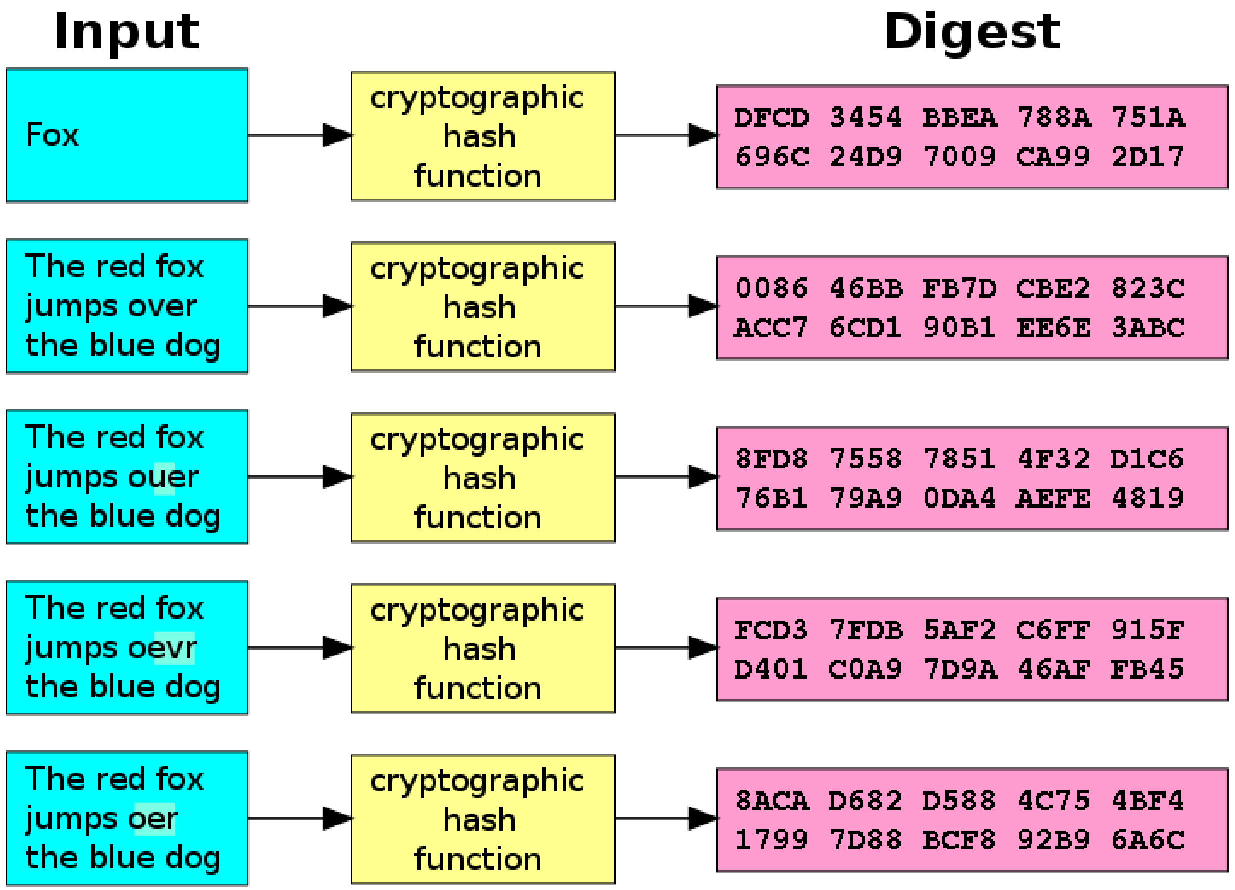
The hash value of the document is a fingerprint of the document.

The main reason is that encrypting the entire document would take too long time (since we are using asymmetric encryption).

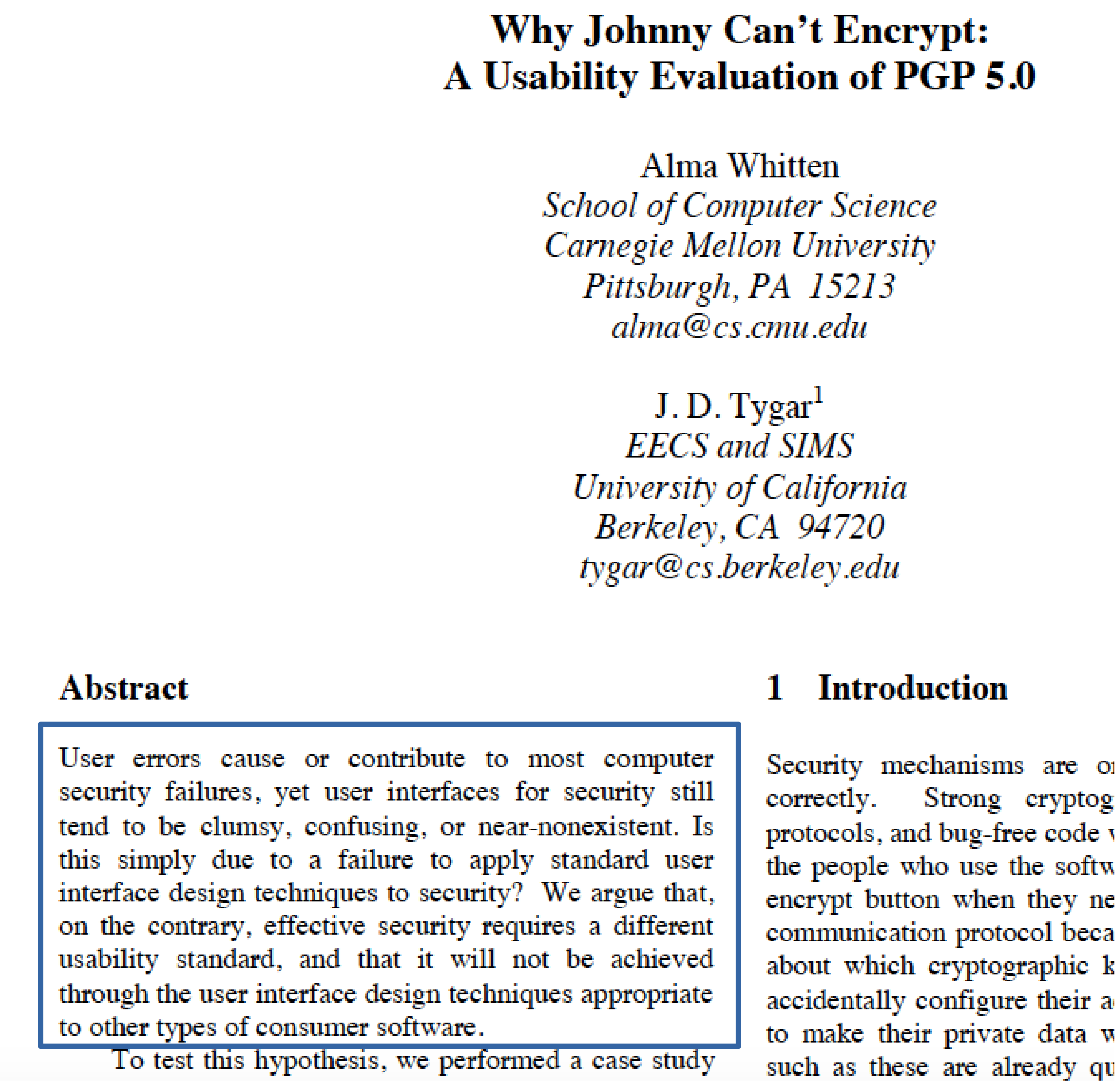
Cryptographic hashing is also used to protect passwords in so-called password files.

Wikipedia:
Cryptographic hash functions have “avalance effect”

Small change in input


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Big change in message digest



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[1]
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 o correctly. Strong cryptog protocols, and bug-free code the people who use the softw encrypt button when they ne communication protocol beca about which cryptographic k accidentally configure their a to make their private data w such as these are already qu